Social Bots und Meinungsbildung in der Demokratie

Patricia Egli*

David Rechsteiner**

Mittels Social Bots – automatisierten Computerprogrammen, die sich in sozialen Netzwerken als Menschen ausgeben – können durch personalisierte Aussagen in potentiell beliebig hoher Anzahl (Falsch-)Informationen verbreitet werden. Social Bots sind daher geeignet, die freie demokratische Meinungsbildung zu beeinflussen. Viele Instrumente des geltenden Rechts erweisen sich im Umgang mit Social Bots als untauglich, da sie auf den jeweiligen Betreiber abzielen, der jedoch fast nicht ermittelt werden kann. Lediglich gestützt auf die Garantie der politischen Rechte, welche auf die Irreführung an sich abstellt, kann ausnahmsweise eine Abstimmung aufgehoben werden. Die Autoren schlagen vor, dass die Behörden gestützt auf ihre bestehenden Informationspflichten über die Risiken von Social Bots aufklären. Weiter ist nach Auffassung der Autoren zu prüfen, ob die Selbstregulierung der Akteure in der demokratischen Meinungsbildung genügt oder zusätzlich staatliche Regulierungsmassnahmen für die sozialen Netzwerke zu ergreifen sind.

Les « social bots », soit des programmes informatiques automatisés qui se font passer pour des personnes sur les réseaux sociaux, permettent de diffuser un nombre potentiellement illimité d'informations (erronées) grâce à des déclarations personnalisées. Les social bots sont donc en mesure d'influencer la libre formation de l'opinion démocratique. De nombreux instruments du droit en vigueur s'avèrent inefficaces pour traiter les social bots puisqu'ils sont dirigés contre leurs exploitants, lesquels ne peuvent quasiment jamais être identifiés. Ce n'est qu'en vertu de la garantie des droits politiques, en invoquant une tromperie du citoyen, qu'il est possible de faire annuler une votation à titre exceptionnel. Les auteurs proposent que les autorités invoquent leur obligation d'information pour rendre les citoyens attentifs aux risques liés aux social bots. Ils estiment par ailleurs qu'il faut examiner si l'autorégulation des acteurs qui contribuent à la formation démocratique de l'opinion suffit ou si l'Etat doit prendre des mesures de régulation supplémentaires pour les réseaux sociaux.

Inhaltsübersicht

I. Einleitung

Die Digitalisierung verändert in zunehmender Weise auch *die demokratischen Abläufe*. Sie erlaubt es grundsätzlich, schneller Informationen auszutauschen und gewährleistet damit eine effizientere Kommunikation, was zu mehr Diskursen und erhöhter Transparenz führen kann. Die Technik erlaubt damit neue Optionen für demokratische Prozesse. So haben die sozialen Medien in neuerer Zeit die demokratische Auseinandersetzung mit sozialen und politischen Themen, beispielsweise im Rahmen des Arabischen Frühlings oder der Bewegung «Occupy Wall Street», bedeutend gestärkt. Jedoch ermöglicht die Digitalisierung neue Kommunikationsformen, zum Beispiel durch den Einsatz von Programmen wie *Social Bots,* die das Potential einer gewissen Beeinträchtigung der freien Meinungsbildung in der Demokratie in sich tragen.

Vor diesem Hintergrund gilt es vorliegend zu diskutieren, welche *Auswirkungen* Social Bots auf die Meinungsbildung in der Demokratie haben können und wie das Recht allenfalls auf diese reagieren soll.

II. Social Bots

Als «Social Bots» werden automatische oder semi-automatische *Computerprogramme* bezeichnet, die sich in sozialen Netzwerken als Menschen ausgeben und/oder

* Patricia Egli, Prof. Dr. iur., LL.M., Assistenzprofessorin für Öffentliches Recht, Völker- und Europarecht an der Universität St. Gallen.

** David Rechsteiner, Dr. iur., Gerichtsschreiber am Verwaltungsgericht des Kantons Bern, Lehrbeauftragter für Bundesstaatsrecht und Selbststudium Privatrecht an der Universität St. Gallen.

Die Autoren danken Prof. Dr. Dirk Helbing, Professor für Computational Social Science an der ETH Zürich, für sein Koreferat an der Tagung zum Roboterrecht und seine wertvollen Hinweise und Anregungen sowie den Tagungsteilnehmerinnen und -teilnehmern für ihre Diskussionsbeiträge.

Die Internetquellen wurden zuletzt am 8.1.2017 besucht.

menschliches Verhalten imitieren.[1] Solche Social Bots verfügen in sozialen Netzwerken über ein Konto, einen Namen, ein Profil und interagieren auf Plattformen wie Twitter, Facebook, Instagram oder Tumblr, aber auch in Youtube-Kommentaren, oft unbemerkt mit Menschen. Sie können anderen Nutzern folgen, Beiträge liken bzw. retweeten, vorgefertigte Nachrichten wiedergeben oder gar selbstständig solche erstellen.[2] Dabei unterscheiden sich ihre Profile und ihr Verhalten, zumindest auf den ersten Blick, kaum von jenem von Menschen, weswegen wir sie nicht als Social Bots erkennen.[3] Es gibt zwar Algorithmen,[4] welche Social Bots aufgrund ihres Verhaltens und ihrer Sprache als solche identifizieren können. Gleichzeitig wird das Verhalten der Bots jedoch raffinierter und menschenähnlicher, was die Entdeckung wiederum erschwert.[5]

Neuere Beispiele zeigen, dass der Einsatz von Social Bots geeignet sein kann, die *freie Meinungsbildung* in Gesellschaften zu steuern und damit demokratische Prozesse zu beeinflussen. Beispielsweise waren Millionen von Twitter-Anhängern von Donald Trump und Hillary Clinton Social Bots, die ungefähr 20 Prozent aller Twitter-Meldungen im Zusammenhang mit den Präsidentschaftswahlen generierten.[6] Social Bots können im Wahlkampf zur Unterstützung, aber auch zur Diffamierung von Kandidierenden eingesetzt werden. Im letzteren Fall wird beispielsweise eine Vielzahl von Tweets mit Hinweisen auf Websites generiert, die Fehlinformationen bzw. sog. «fake news» über Kandidierende verbreiten. Je häufiger eine solche Falschmeldung von echten Benutzern geteilt und in anderen sozialen Netzwerken verbreitet wird, desto mehr Glaubwürdigkeit erhält sie und desto eher beginnen Menschen, sich in ihrer Meinungsbildung danach zu richten.[7] Eine Analyse von Twitter-Profilen der vier grossen Schweizer Parteien hat wiederum ergeben, dass 15 bis 40 Prozent aller Follower Bots oder inaktive User sind.[8] Und bezüglich der Debatte um den EU-Austritt in Grossbritannien besteht der Verdacht, dass ein Drittel aller Twitter-Meldungen von Social Bots verfasst wurden, die mehrheitlich den Austritt befürworteten.[9] In diesem Zusammenhang ist denn auch von «influence bots»[10] oder von einem «Bot-Effekt»[11] die Rede.

Im *Unterschied zu herkömmlicher Beeinflussung* der Meinungsbildung durch Inserate, Flugblätter oder Aussagen im Rahmen politischer Versammlungen besteht bei der Beeinflussung im Rahmen der sozialen Netzwerke mit Social Bots die Möglichkeit, mehrfach personalisierte Aussagen, d.h. Aussagen im Namen einer Vielzahl von fiktiven Personen, machen zu können. So haben beispielsweise im US-Wahlkampf viele Twitter-Nutzer mit spanischen Namen Donald Trump gelobt. Später stellte sich heraus, dass es diese Personen gar nicht gab.[12] Mit einer Vielzahl von personalisierten Beiträgen und den darin eingebetteten Links, Bildern und Videos, die auch in anderen sozialen Netzwerken verbreitet werden, kann auf eine Debatte mit immer grösserer Glaubwürdigkeit einge-

---

1 Vgl. Claudia Wagner/Silvia Mitter/Christian Körner/Markus Strohmaier, When social bots attack: Modeling susceptibility of users in online social networks, in: Matthew Rowe/Milan Stankovic/Aba-Sah Dadzie (Hrsg.), Proceedings of the 2nd Workshop on Making Sense of Microposts (MSM2012), 41–48; Emilio Ferrara/Onur Varol/Clayton Davis/Filippo Menczer/Alessadro Flammini, The Rise of Social Bots, Communications of the ACM, Vol. 59, No. 7, 96–104; Alessandro Bessi/Emilio Ferrara, Social bots distort the 2016 U.S. Presidential election online discussion, First Monday, Vol. 21, No. 11, 7.11.2016, Internet: http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653.
Zum Begriff «Bot» (im Gegensatz zum «Roboter») siehe Isabelle Wildhaber/Melinda F. Lohmann, Roboterrecht – eine Einleitung, AJP 2017, 135 ff., 135 f.

2 Martin Fuchs, Automatisierte Trolle, Warum Social Bots unsere Demokratie gefährden, NZZ vom 12.9.2016, Internet: http://www.nzz.ch/digital/automatisierte-trolle-warum-social-bots-unsere-demokratie-gefaehrden-ld.116166.

3 Gordana Mijuk, Hier spricht ein Roboter, NZZ am Sonntag vom 28.8.2016, 20.

4 So beispielsweise http://truthy.indiana.edu/botornot/.

5 Vgl. Melanie Amann/Horand Knaup/Ann-Katrin Müller/Marcel Rosenbach/Wolf Wiedmann-Schmidt, Social Bots, Wie digitale Dreckschleudern Meinung machen, Der Spiegel, Ausg. 43, 22. Oktober 2016, 44–45; Ferrara et al. (FN 1), 103; Fuchs (FN 2); Oliver Georgi, Software-Roboter, Automatisierter Hass im Netz, Frankfurter Allgemeine vom 24.5.2016, Internet: http://www.faz.net/-gpf-8hc5h; allgemein dazu vgl. Dirk Helbing et al., Das Digital-Manifest, Spektrum der Wissenschaft, 17.12.2015, Internet: http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933.

6 Bessi/Ferrara (FN 1); Stefan Betschon, Die dunkle Macht der Algorithmen, NZZ vom 24.11.2016, 7; Simon Hegelich, Invasion der Meinungsroboter, in: Konrad-Adenauer-Stiftung e.V. (Hrsg.), Analysen & Argumente, Ausg. 221, Berlin 2016, 1–9; Joachim Laukenmann, Wie digitale Medien Wähler manipulieren, Sonntagszeitung vom 10. April 2016, Internet: http://www.sonntagszeitung.ch/read/sz_10_04_2016/gesellschaft/Wie-digitale-Medien-Waehler-manipulieren-59964; Mijuk (FN 3), 20.

7 Ferrara et al. (FN 1), 98 f.; vgl. auch Jacob Ratkiewicz/Michael D. Conover/Martin Meiss/Bruno Gonçalves/Alessandro Flammini/Filippo Menczer, Detecting and tracking political abuse in social media, Proceedings of the 5th International AAAI Conference on Weblogs and Social Media 2011, 297–304.

8 Vgl. Laukenmann (FN 6).

9 Mijuk (FN 3), 20; vgl. dazu differenzierend Hegelich (FN 6), 4 f.

10 V.S. Subrahmanian et al., The DARPA Twitter Bot Challenge, 21.4.2016, Internet: https://arxiv.org/pdf/1601.05140v2.pdf.

11 Hegelich (FN 6), 4.

12 Mijuk (FN 3), 20 f.; Matthias Schüssler, Sie sind schon unter uns, Tages-Anzeiger vom 11.5.2016, 33.

wirkt werden. Denn je öfter eine Thematik in den sozialen Netzwerken diskutiert wird, desto relevanter erscheint sie auch. Wenn Tausende von Social Bots eine Frage immer wieder aufnehmen und ähnliche Beiträge verbreiten, können sie einen bestimmten Trend setzen. Dieser beeinflusst wiederum die Handlungen von natürlichen Personen, die sich in ihrer Arbeit auf Analysen der sozialen Netzwerke stützen.[13]

Problematisch ist weiter, dass es generell schwierig ist, Social Bots überhaupt als solche zu *identifizieren*. Bereits heute gibt es Bots mit künstlicher Intelligenz. Sie verstehen Sprache, können mit Menschen kommunizieren und sich weiterentwickeln.[14] Weiter ist es praktisch nicht möglich, den Betreiber eines Social Bots oder gar eines Netzwerks solcher Programme ausfindig zu machen.[15] Dazu kommt, dass die Rechtsdurchsetzung im Internet generell schwierig ist, da sich die notwendigen Daten häufig im Ausland befinden.[16] Diese Manipulationen können grundsätzlich auch von menschlichen Trollen vorgenommen werden. So betreibt beispielsweise Russland sogenannte Troll-Fabriken mit Hunderten von Mitarbeitern.[17] Die besondere Problematik bei Social Bots im Vergleich zu menschlichen Trollen besteht darin, dass erstere günstig und fast beliebig skalierbar sind, d.h. ihre Anzahl mit zusätzlichem Mitteleinsatz proportional erhöht werden kann.[18] Zur «Herstellung» von Social Bots benötigt es lediglich Nutzerkonten des jeweiligen sozialen Netzwerks, Zugriff auf eine automatisierte Schnittstelle (API) dieses Netzwerks sowie eine Steuerungssoftware. Preislich sollen 10'000 falsche Twitter-Nutzerkonten mit dazugehöriger Steuerungssoftware bereits ab USD 1'000 erhältlich sein.[19]

III. Rechtliche Rahmenbedingungen

Die Beeinflussung der politischen Meinungsbildung wird hauptsächlich von der Garantie der politischen Rechte erfasst. Diese ist auch bei einer allfälligen Beeinflussung durch Social Bots einschlägig. Daneben werden weitere Gesetze angeschaut, welche von Belang sein könnten.

A. Garantie der politischen Rechte

Die Garantie der politischen Rechte umfasst gemäss *Art. 34 Abs. 2 BV* die freie Willensbildung und die unverfälschte Stimmabgabe. Demnach soll kein Wahl- oder Abstimmungsergebnis anerkannt werden, welches nicht «den freien Willen der Stimmbürger zuverlässig und unverfälscht zum Ausdruck bringt».[20] Neben den Anforderungen an das Verfahren und dem Anspruch auf richtige Ermittlung des Wahl- bzw. Abstimmungsergebnisses umfasst die Garantie der politischen Rechte auch die Gewährleistung des Stimmgeheimnisses, den Schutz der Einheit der Materie sowie den Schutz vor unzulässiger Einflussnahme.[21] Letzterer kann betroffen sein, wenn durch den Einsatz von Social Bots falsche Informationen verbreitet werden. In welchen Fällen eine Einflussnahme unzulässig ist, hängt davon ab, ob diese von den Behörden (III.A.1.) oder von Privaten (III.A.2.) ausgeht.

1. Einflussnahme der Behörden

Die Behörden dürfen im Vorfeld von *Abstimmungen,* beispielsweise im Rahmen der Abstimmungserläuterungen, Vorlagen erklären und zur Annahme oder Ablehnung empfehlen. Dabei sind sie nicht zur Neutralität, aber zur Sachlichkeit verpflichtet.[22] Während des eigentlichen Abstimmungskampfs wurde eine behördliche Einflussnahme früher nur ausnahmsweise beim Vorliegen von triftigen Gründen erlaubt.[23] Heute sind die Voraussetzungen für ein

---

13 Vgl. Hegelich (FN 6), 3 f.; allgemein zum «Echokammereffekt» und der «Filter Bubble» im Internet vgl. Helbing et al. (FN 5).

14 Mijuk (FN 3), 21, mit Hinweis auf das von Microsoft lancierte Experiment mit Tay; Ferrara et al. (FN 1), 99 f. m.w.H.; Fuchs (FN 2); Hegelich (FN 6), 7; Christian Meier/Jennifer Wilton, Maschinen übernehmen die Macht im Internet, Die Welt vom 11.4.2016, Internet: https://www.welt.de/wirtschaft/webwelt/article154223388/Maschinen-uebernehmen-die-Macht-im-Internet.html; vgl. auch Subrahmanian et al. (FN 10), 2 ff.

15 Meike Laaff, Datenexperte über Social Bots, «Manipulation ist nicht so einfach» [Interview mit Prof. Simon Hegelich], taz. die tageszeitung vom 21.9.2016, Internet: http://www.taz.de/!5337164/; Mijuk (FN 3), 20; vgl. auch Bessi/Ferrara (FN 1).

16 Da viele Länder keine oder nur eine kurze Vorratsdatenspeicherung kennen, sind die erforderlichen ausländischen Daten bei der Bearbeitung des Rechtshilfeersuchens häufig bereits nicht mehr vorhanden, weswegen die gesuchten Personen unerkannt bleiben; siehe statt vieler Sandra Schweingruber, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10.11.2014, N 5; Georgi (FN 5).

17 Roman Rey, Insiderin packt aus – so läuft es in Putins Troll-Fabrik wirklich, watson.ch, 9.4.2015, Internet: http://wat.is/-yQxWgqhD; Christian Weisflog, Putins Internetpiraten, NZZ vom 18.6.2014, 5.

18 Hegelich (FN 6), 2; Schüssler (FN 12), 33.

19 Vgl. Hegelich (FN 6), 2 f.; vgl. auch Bessi/Ferrara (FN 1).

20 Statt vieler BGE 141 II 297 E. 5.2; BGer, 1C_210/2016, 24.8.2016, E. 3.2.

21 BSK BV-Tschannen, Art. 34 N 32, in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015 (zit. BSK BV-Verfasser).

22 BGE 138 I 61 E. 6.2, 135 I 292 E. 4.2; BGer, 1C_455/2016, 14.12.2016, E. 4.4.

23 BGE 119 Ia 271 E. 3b, 114 Ia 427 E. 4c.

behördliches Engagement im Abstimmungskampf weniger streng. Es wird jedoch verlangt, dass ein solches sachlich und transparent erfolgt sowie in verhältnismässiger Weise zur offenen Meinungsbildung beiträgt.[24] Da eine Einflussnahme der Behörden mittels Social Bots intransparent ist, wäre eine solche wohl *per se* unzulässig.

Anders als bei Abstimmungen dürfen die Behörden bei *Wahlen* keine Empfehlungen abgeben oder anderweitig in den Wahlkampf eingreifen.[25] Damit scheidet ein Einsatz von Social Bots erst recht aus.

Einen besonderen Fall der behördlichen Intervention stellt die *Richtigstellung* von irreführenden Informationen dar, welche von Privaten verbreitet wurden. Ein solches Eingreifen der Behörden ist nicht nur zulässig, sondern gar geboten und kann eine schwerwiegende Irreführung verhindern.[26]

Bei einem *Verstoss* gegen diese Schranken kann die entsprechende Abstimmung oder Wahl aufgehoben werden. Vorausgesetzt wird, dass eine Beeinflussung des Ergebnisses im Bereich des Möglichen liegt. Sofern die Auswirkungen der behördlichen Einflussnahme nicht ziffernmässig festgestellt werden können, sind sie mit Blick auf die Grösse des Stimmenunterschiedes, nach der Schwere des Mangels und dessen Bedeutung für die Abstimmung als Ganzes zu beurteilen. «Erscheint die Möglichkeit, dass die Abstimmung ohne den Mangel anders ausgefallen wäre, nach den gesamten Umständen [nicht] als derart gering, dass sie nicht mehr ernsthaft in Betracht fällt», so ist die Abstimmung aufzuheben,[27] soweit nicht aus Gründen der Rechtssicherheit davon abzusehen ist.[28]

2. Einflussnahme von Privaten

Der Prozess der politischen Meinungsbildung soll durch die gesellschaftlichen Akteure und damit durch Private vorgenommen werden. Die Einflussnahme von Privaten ist *erwünscht* und durch die Kommunikationsgrundrechte geschützt.[29] Deswegen wird auf Einschränkungen fast vollständig verzichtet. Übertreibungen und sogar Unwahrheiten werden in Kauf genommen, und es wird den Stimmberechtigten zugetraut, diese als solche zu erkennen und sich ein entsprechendes Urteil zu bilden.[30] Nur in zwei Fällen bzw. Fallgruppen ist eine private Einflussnahme verfassungswidrig: Bei Verwendung eines unzulässigen Mittels (z.B. Drohung) sowie bei schweren Irreführungen.[31]

a. Unzulässige Einflussmittel

Eine private Einflussnahme ist immer dann unzulässig, wenn sie sich eines unzulässigen Mittels bedient. Als solches kommen *Einschüchterungen, Drohungen, Gewaltanwendungen und Bestechung* in Frage.[32] Diese Handlungen sind ein Verstoss gegen Art. 34 Abs. 2 BV. Ist es sicher oder sehr wahrscheinlich, dass dadurch das Abstimmungsergebnis in entscheidender Weise beeinflusst wurde, so ist die Abstimmung aufzuheben.[33] Darüber hinaus verstossen solche Handlungen auch gegen die Bestimmungen des vierzehnten Titels des Schweizerischen Strafgesetzbuches,[34] welche Ausfluss der grundrechtlichen Schutzpflicht für die politischen Rechte sind.[35]

Da die Verwendung von unzulässigen Einflussmitteln grundsätzlich nicht zur besonderen Problematik der Social Bots gehört und überdies auch *keine entsprechenden Fälle* bekannt sind, ist diese Thematik vorliegend nicht weiter von Interesse.

---

[24] Art. 10a Abs. 2 Bundesgesetz vom 17. Dezember 1976 über die politischen Rechte (BPR; SR 161.1); BGer, 1C_412/2007, 18.7.2008, E. 6.2; vgl. auch BGE 140 I 338 E. 5.1 sowie ausführlich Pierre Tschannen, Staatsrecht der schweizerischen Eidgenossenschaft, 4. A., Bern 2016, § 52 N 1 ff., insb. 12.

[25] BGE 124 I 55 E. 2a; BGer, 1C_522/2015, 1C_527/2015 und 1C_535/2015, 29.10.2015, E. 4.3.2; vgl. Gerold Steinmann, Art. 34 BV N 22, in: Bernhard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. A., Zürich/St. Gallen 2014 (zit. SG BV-Komm-Verfasser).

[26] Tschannen (FN 24), § 52 N 13 f.; vgl. BGer, 1C_472/2010, 20.1.2011, E. 5; vgl. unten III.A.2.b.

[27] BGE 135 I 292 E. 4.4; sowie BGE 138 I 61 E. 4.7.2, 132 I 104 E. 3.3; BGer, 1C_152/2014, 27.8.2014, E. 2.3; Tschannen (FN 24), § 48 N 47.

[28] BGE 138 I 61 E. 4.7.3; BSK BV-Tschannen (FN 21), Art. 34 N 54.

[29] Vgl. Yvo Hangartner/Andreas Kley, Die demokratischen Rechte in Bund und Kantonen der Schweizerischen Eidgenossenschaft, Zürich 2000, N 2664; Pierre Tschannen, Schutz der politischen Rechte, in: Detlef Merten/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band VII/2: Grundrechte in der Schweiz und in Liechtenstein, Heidelberg 2007, 491–516, N 59 u. 69 f.

[30] Vgl. BGE 135 I 292 E. 4.1, 119 Ia 271 E. 3c, 98 Ia 73 E. 3b; BGer, 1C_472/2010, 20.1.2011, E. 4; Tschannen (FN 24), § 52 N 27.

[31] Michel Besson, Behördliche Informationen vor Volksabstimmungen, Verfassungsrechtlichen Anforderungen an die freie Willensbildung der Stimmberechtigen in Bund und Kantonen, Diss. Bern 2002, 357.

[32] Besson (FN 31), 358 ff.

[33] Vgl. auch unten III.A.2.b. a.E.

[34] Vgl. unten III.B.

[35] Vgl. Andreas Kley, Politische Rechte, in: Giovanni Biaggini/Thomas Gächter/Regina Kiener (Hrsg.), Staatsrecht, 2. A., Zürich/St. Gallen 2015, 585–661, N 81; SG BV-Komm-Schweizer (FN 25), Art. 35 BV N 51; BSK StGB II-Wehrle, vor Art. 279 N 5, in: Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111–392 StGB, 3. A., Basel 2013.

b. Schwerwiegende Irreführung

Der zweite Fall der unzulässigen Einflussnahme durch Private ist die schwere Irreführung der Stimmberechtigten. Ob eine solche vorliegt, wird anhand von *vier Voraussetzungen* geprüft.[36] Sind diese erfüllt, so wird die entsprechende Abstimmung oder Wahl grundsätzlich aufgehoben bzw. wiederholt.[37] Wie bei einer behördlichen Beeinflussung kann allenfalls aus Gründen der Rechtssicherheit davon abgesehen werden.[38]

Als erstes wird vorausgesetzt, dass es sich bei der Irreführung um eine *Tatsachenbehauptung* und nicht um ein Werturteil handelt.[39] Beim Einsatz von Social Bots ist dabei zu bedenken, dass ein Social Bot jeweils vorgibt, ein echter Mensch zu sein und damit auch bei der Abgabe eines Werturteils gleichzeitig über eine Tatsache täuscht.

Zweitens muss die Irreführung schwerwiegend sein. Das heisst, die fragliche Tatsache muss für den *Entscheid wesentlich* sein oder den *Kern der Vorlage* anbelangen und beim Stimmbürger ein falsches Bild auslösen.[40] Dabei ergeben sich beim Einsatz von Social Bots derzeit keine Besonderheiten. Man kann sich jedoch fragen, ob mit zusätzlichem Auftreten von Social Bots und dem Bekanntwerden der Problematik nicht künftig (stärker) davon ausgegangen werden muss, dass Informationen in sozialen Netzwerken, welche ursprünglich von Personen, welche man nicht persönlich kennt, stammen, generell als unzuverlässig gelten müssen, weswegen nicht mehr von einer schwerwiegenden Irreführung gesprochen werden könnte. Zumindest zurzeit dürfte dies aber nicht der Fall sein.

Drittens wird gefordert, dass die Irreführung *kurz vor der Abstimmung* stattfindet und so die Richtigstellung durch andere Private oder die Behörden verunmöglicht wird.[41] Das Verbot der schwerwiegenden Irreführung durch Private wird deswegen teilweise auch als Überrumpelungsverbot bezeichnet.[42] Bei Abstimmungen, bei welchen die Möglichkeit der brieflichen Stimmabgabe besteht, wird dieses Kriterium von Michel Besson kritisiert. Er bemängelt, dass der Zeitpunkt kurz vor der Abstimmung nicht relevant sei, da viele Stimmbürger ihre Stimme bereits brieflich abgegeben hätten. Grundsätzlich könne eine irreführende Tatsachenbehauptung während der ganzen Zeit, in welcher brieflich abgestimmt werden kann, relevant sein. Allerdings werde, da kurz nach der Irreführung jeweils nur ein Teil der Stimmbürger abstimmen würden, eine private Information fast nie einen entscheidenden Einfluss auf das Abstimmungsergebnis haben.[43] Das Bundesgericht hat diese Bedenken aufgegriffen, die Frage jedoch offengelassen.[44]

Besson ist insofern zuzustimmen, als dass jede private Irreführung zwischen Erhalt des Stimmcouverts und dem Abstimmungstag eine unzulässige Beeinflussung der freien Willensbildung darstellen kann. Allerdings impliziert die Schlussfolgerung, dass jede falsche Tatsache innert kurzer Zeit richtiggestellt werden kann. Es besteht aber auch die Möglichkeit, dass eine Information zwar klarerweise falsch ist, dies jedoch erst nach einiger Zeit erkannt und richtiggestellt werden kann. Unseres Erachtens ist deshalb darauf abzustellen, wie lange eine Irreführung, ohne als solche erkannt zu werden, im Raum stand und wie viele Stimmberechtige während dieser Zeit von ihrem Stimmrecht Gebrauch gemacht haben.

Schliesslich wird als vierte Voraussetzung verlangt, dass es sicher oder zumindest sehr wahrscheinlich ist, dass die Irreführung eine *entscheidende Auswirkung* auf das Ergebnis der Abstimmung oder Wahl hatte.[45] Die Schwelle für eine Aufhebung oder Wiederholung einer Abstimmung oder Wahl ist damit höher als bei einer Beeinflussung durch die Behörden.[46] Bezüglich Social Bots ist zu bedenken, dass diese einerseits nicht einfach zu erkennen sind und andererseits ihr Einfluss auf das Stimmverhalten kaum festzustellen ist.[47]

B. Weitere Gesetze

Die *Vergehen gegen den Volkswillen* sind im vierzehnten Titel des Strafgesetzbuches geregelt (Art. 279–283 StGB). Diese Tatbestände schützen schwergewichtig die Ausübung des Stimm- und Wahlrechts, nicht aber die Meinungsbildung im Vorfeld der Abstimmung.[48] Somit

---

36 Hangartner/Kley (FN 29), N 2670 ff.; vgl. auch Besson (FN 31), 361 f., welcher die ersten beiden Voraussetzungen zusammen behandelt.
37 BGE 135 I 292 E. 4.1, 119 Ia 271 E. 3c.
38 Vgl. oben III.A.1.
39 Hangartner/Kley (FN 29), N 2671.
40 BGer, 1C_472/2010, 20.1.2011, E. 4.
41 BGE 135 I 292 E. 4.1; vgl. Hangartner/Kley (FN 29), N 2673.
42 BSK BV-Tschannen (FN 21), Art. 34 N 38.
43 Besson (FN 31), 365.
44 BGer, 1C_472/2010, 20.1.2011, E. 5. Es wurde lediglich ausgeführt, dass im konkreten Fall eine behördliche Richtigstellung von falschen privaten Informationen für Personen, die in einem frühen Stadium brieflich abgestimmt haben, zu spät gekommen wäre.
45 BGE 119 Ia 271 E. 3c; Besson (FN 31), 362.
46 Hangartner/Kley (FN 29), N 2674; BSK BV-Tschannen (FN 21), Art. 34 N 54.
47 Laaff (FN 15).
48 So BGE 103 IV 157 E. 3. Auch der einschlägig klingende § 108a (Wählertäuschung) des deutschen StGB (Strafgesetzbuch vom 15. Mai 1871, in der Fassung der Bekanntmachung vom 13. November 1998 [BGBl. I S. 3322]) schützt nicht die Willensbildung, sondern die Willenserklärung; siehe statt vieler Dieter Anders/

werden die geschilderten Aktivitäten von Social Bots von ihnen nicht erfasst.

Einen gewissen Schutz vor Irreführungen durch Social Bots bietet hingegen der zivil- und strafrechtliche *Ehrenschutz*.[49] Dieser untersagt unwahre Tatsachenbehauptungen, soweit sie einzelne Personen betreffen. Zivil- und strafrechtlich verantwortlich macht sich dabei der Betreiber der Social Bots. Dieser ist jedoch wie erwähnt praktisch nicht zu eruieren.[50] Dasselbe Problem stellt sich bei weiteren Straftatbeständen, welche je nach Art der Aussage der Social Bots einschlägig sein können.[51]

Die Äusserungen von Social Bots könnten als Massenwerbung angesehen werden, welche grundsätzlich vom *UWG*[52] erfasst wird. Der Anwendungsbereich des UWG umfasst jedoch nur wirtschaftliche Wettbewerbshandlungen. Das Verhalten im politischen Rahmen, insbesondere der Wahl- und Abstimmungskampf, fällt nicht darunter.[53]

C. Zwischenfazit

Social Bots haben das *Potential,* die politische Meinungsbildung zu beeinflussen. Ob dieser Einfluss jedoch tatsächlich in schwerwiegender Weise irreführend ist und dadurch schlussendlich das Ergebnis einer Wahl oder einer Abstimmung verändert wird, ist schwer zu eruieren. Ein erstes Problem im Zusammenhang mit Social Bots besteht darin, sie überhaupt zu entdecken. Noch schwieriger ist festzustellen, welche natürlichen Personen hinter dem Einsatz von Social Bots stehen.[54] Die Effekte von Social Bots sind zudem schwierig zu messen. Oftmals ist es ja nicht lediglich ein Beitrag, sondern gerade die Möglichkeit, mit einer Vielzahl von personalisierten Beiträgen, die auch in anderen sozialen Netzwerken verbreitet werden, auf eine Debatte mit immer grösserer Glaubwürdigkeit einzuwirken und damit Trends zu setzen.

Vor diesem Hintergrund bieten die vorhandenen Straftatbestände keinen auch nur annähernden Schutz gegen die Beeinflussung der Meinungsbildung durch Social Bots. Sie bedingen die Identifikation des Betreibers eines Social Bots oder eines ganzen Netzwerks, was fast unmöglich ist. Anders die Garantie der politischen Rechte, welche die Meinungsbildung auch ohne Kenntnis des Urhebers von Falschinformationen schützt. Dafür statuiert diese lediglich, dass eine Abstimmung oder eine Wahl nicht anerkannt wird, wenn das Ergebnis sehr wahrscheinlich beeinflusst wurde. Wurde beispielsweise lediglich der Anteil der Ja- oder Nein-Stimmen einer Sachvorlage, ohne Änderung des Ergebnisses, beeinflusst, so bietet Art. 34 Abs. 2 BV keine Handhabe. Dies ist *unbefriedigend,* da auch in diesem Fall Meinungen beeinflusst wurden und sich diese Beeinflussung an anderer Stelle, beispielsweise bei einer nächsten Abstimmung, bei der Ausübung des passiven Wahlrechts oder im Verhalten in Wirtschaft und Gesellschaft, manifestieren kann.

IV. Handlungsoptionen

A. Ausgangslage

Bei den Social Bots geht es um ein *Risiko,* dessen Schadens- und Wirkungsverläufe nicht vollständig bekannt sind. Aus rechtsdogmatischer Sicht bedeutet dies, dass mögliche rechtliche Handlungsoptionen unter Ungewissheitsbedingungen diskutiert werden müssen. Solche Situationen erfordern besondere Informationsverarbeitungskapazitäten sowie kontinuierliche Lern- und Anpassungsprozesse.[55] Insbesondere gilt es zu überlegen, mit welchen Massnahmen die unterschiedlichen Akteure der demokratischen Meinungsbildung schrittweise auf die Problematik sensibilisiert und allenfalls welche Aspekte rechtlich normiert werden sollen.

Zu berücksichtigen gilt es dabei, dass die Risiken der Bot-Technik im Bereich der sozialen Netzwerke nicht losgelöst von deren *Chancen* diskutiert werden sollten.[56] Neue Technologien bergen ja nicht nur Gefährdungen, sondern stellen auch immer Innovationsleistungen dar, die auch von der Verfassung angestrebte Wohlfahrtsaspekte realisieren.[57] Ziel ist es daher, die Risiken mit staatlichen Massnahmen wirksam auf ein sozialadäquates Mass zu

---

Markus Mavany, in: Klaus Leipold/Michael Tsambikakis/Mark A. Zöller (Hrsg.), AnwaltKommentar StGB, 2. A., Heidelberg 2015, § 108a N 4 m.w.H.

49 Art. 28 ZGB; Art. 173–178 StGB.

50 Vgl. oben II.

51 Zu denken ist beispielsweise an Rassendiskriminierung (Art. 261bis StGB).

52 Bundesgesetz vom 19. Dezember 1986 gegen den unlauteren Wettbewerb (UWG; SR 241).

53 BGer, 6B_188/2013, 4.7.2013, E. 6.3; Lucas David/Reto Jacobs, Schweizerisches Wettbewerbsrecht, 5. A., Bern 2012, N 24.

54 Vgl. Ferrara et al. (FN 1), 103; Mijuk (FN 3), 20.

55 Peter Hettich, Kooperative Risikovorsorge, Regulierte Selbstregulierung im Recht der operationellen und technischen Risiken, Zürich/Basel/Genf 2014, N 27; Christoph Errass, Technikregulierung zur Gewährleistung von Sicherheit, S&R 2016, 62–89, 82 ff.; Alexander Ruch, Regulierungsfragen der Gentechnologie und des Internet, ZSR 123 (2004) II, 373–475, 392, 410.

56 Für Beispiele von Bots vgl. Ian R. Kerr, Bots, Babes and the Californication of Commerce, University of Ottawa Law and Technology Journal, Vol. 1, 2004, 284–324, 306 ff. Für Anwendungsfelder der Bot-Technik vgl. beispielsweise https://www.botanicalls.com/kits/; https://meekan.com/; https://digit.co/; https://pana.com.

57 Hettich (FN 55), N 31; Ruch (FN 55), 400.

begrenzen. Dieses Mass bestimmt sich auch danach, wie weit mit dem Einsatz von rechtlich bereits vorgesehen Informationspflichten des Staates eine Sensibilisierung der Akteure im demokratischen Prozess erreicht werden kann und ob bereits Ansätze zur Selbstregulierung vorhanden sind, die ein weiteres staatliches Eingreifen nicht notwendig erscheinen lassen.[58]

B. Informationspflichten

Der Staat kann zunächst mit dem Instrument der *Realakte* versuchen, eine Sensibilisierung für die durch Social Bots hervorgerufenen Herausforderungen zu erreichen. Realakte führen unmittelbar einen Taterfolg herbei und sind entsprechend nicht auf Rechtswirkungen gerichtet.[59] Zu den Realakten gehören insbesondere die Informationspflichten der Behörden.

Informationspflichten umfassen zum einen die Berichterstattung über die behördliche Tätigkeit.[60] Beispielsweise hat der Bundesrat gemäss Art. 180 Abs. 2 BV die Öffentlichkeit rechtzeitig und umfassend über seine Tätigkeit zu informieren, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen. Art. 10 Abs. 2 RVOG[61] konkretisiert, dass der Bundesrat für eine einheitliche, frühzeitige und kontinuierliche Information über seine Lagebeurteilung, Planungen, Entscheide und Vorkehren sorgt. Gestützt auf diese Bestimmungen könnte der Bundesrat die Thematik der Social Bots und deren potentiellen Einfluss auf die freie Meinungsbildung ganz generell thematisieren, was zur Sensibilisierung der Öffentlichkeit beitragen würde.[62] Die Information über das Risiko einer Beeinflussung durch Social Bots könnte weiter mit einer Empfehlung verbunden werden, sich über verschiedene Kanäle zu informieren, bei Auffälligkeiten in sozialen Netzwerken mit bestimmten Fragestellungen zu versuchen, Social Bots zu erkennen[63] oder aber die Betreiber der sozialen Netzwerke zu kontaktieren und Beanstandungen zu melden.

Zum anderen beziehen sich Informationspflichten der Behörden auf die Berichterstattung über Sachprobleme in deren Zuständigkeitsbereich. So informiert der Bundesrat gestützt auf Art. 10a Abs. 1 BPR die Stimmberechtigten kontinuierlich über die eidgenössischen Abstimmungsvorlagen. Er beachtet dabei die Grundsätze der Vollständigkeit, der Sachlichkeit, der Transparenz und der Verhältnismässigkeit (Art. 10a Abs. 2 BPR). Ist mit Blick auf *konkrete Abstimmungen* auf Bundesebene festzustellen, dass aufgrund des Einsatzes von Social Bots in den sozialen Netzwerken eine Beeinträchtigung der freien Willensbildung droht, so umfasst die Informationspflicht des Bundesrates gerade aufgrund der Prinzipien der Vollständigkeit und der Transparenz, die Stimmberechtigten auf dieses Risiko hinzuweisen. In Bezug auf Wahlen bestimmt Art. 34 BPR weiter, dass die Bundeskanzlei vor jeder Gesamterneuerungswahl eine kurze Wahlanleitung erstellt, die den Stimmberechtigten der Kantone mit Verhältniswahl zusammen mit den Wahlzetteln zugestellt wird. Denkbar wäre, dass in dieser Wahlanleitung ebenfalls auf Risiken in Bezug auf Social Bots hingewiesen werden könnte. Sind auf kantonaler Ebene vergleichbare Informationspflichten der Behörden mit Blick auf Wahlen und Abstimmungen vorhanden, so sind auch diese gehalten, auf die Gefährdung der Meinungsbildung durch Social Bots hinzuweisen und entsprechende Empfehlungen zu formulieren.

C. Selbstregulierung

1. Soziale Netzwerke

Neben den Informationspflichten der Behörden stellt sich die Frage, ob aufgrund des Einsatzes von Social Bots in sozialen Netzwerken die entsprechenden Unternehmen

---

58 Im Rahmen des Internet-Rechts haben sich unter den Netzteilnehmern beispielsweise schon früh Verhaltensregeln entwickelt, die als Netiquette bezeichnet werden. Vgl. von der Intel Corporation Sally Hambridge, Netiquette Guidelines, Santa Clara CA, Oktober 1995, Internet: https://www.ietf.org/rfc/rfc1855.txt. Allgemein zur Internet Governance vgl. beispielsweise das Internet Governance Forum (IGF) der UNO sowie der Europäische Dialog zur Internet Gouvernanz (EuroDIG).

59 Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 7. A., Zürich/St. Gallen 2016, N 1408 ff.; Pierre Moor/Etienne Poltier, Droit administratif II, 3. A., Bern 2011, 28, 31 f.; Pierre Tschannen/Ulrich Zimmerli/Markus Müller, Allgemeines Verwaltungsrecht, 4. A., Bern 2014, § 38 N 1, 4.

60 Dazu etwa Pascal Mahon, L'information par les autorités, ZSR 118 (1999) II, 199–352, 250 ff.; Pierre Tschannen, Amtliche Warnungen und Empfehlungen, ZSR 118 (1999) II, 353–455, 364 f.; zur Notwendigkeit der Wissenschaftskommunikation sodann Ruch (FN 55), 398.

61 Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG; SR 172.010).

62 Der Bundesrat hat in Bezug auf Social Bots noch keine Informationen veröffentlicht. Bei den eidgenössischen Wahlen 2015 wurde weder über die Gefahr von unzulässiger Einflussnahme auf die Willensbildung der Stimmberechtigten im Allgemeinen noch über jene von Social Bots im Besonderen informiert (Internet: https://www.ch.ch/de/wahlen2015; Bundeskanzlei [Hrsg.], Wahlanleitung für die Nationalratswahlen vom 18. Oktober 2015, Bern 2015).

63 Vgl. Sebastian Jabbusch, Wie ich einmal mit einer Maschine flirtete, Bento, 25. Mai 2016, Internet: http://www.bento.de/gadgets/fake-profile-auf-facebook-wie-ich-mit-einem-social-bot-flirtete-584991/.

bereits selber reagiert und Massnahmen ergriffen haben, die einer Selbstregulierung[64] der Branche entsprechen würde. Die einzelnen sozialen Netzwerke verfügen zwar über *Regeln und Richtlinien für ihre Benutzer,*[65] die es zum Teil auch explizit untersagen, mittels Bots auf die Netzwerke zuzugreifen.[66] Zudem haben Facebook und Google nach heftiger Kritik im Zusammenhang mit den Präsidentschaftswahlen in den Vereinigten Staaten angekündigt, verstärkt gegen das Verbreiten von Fehlinformationen vorzugehen.[67] Facebook arbeitet beispielsweise an besseren technischen Mitteln zur Entdeckung von falschen Informationen, an einfacheren Meldesystemen für die Benutzer und auch an Warnhinweisen bei Fehlinformationen.[68] In Bezug auf Social Bots existieren jedoch noch keine «Codes of Conduct», die ein effektives branchenweites Vorgehen festlegen würden. Die Erarbeitung solcher Regeln für die sozialen Netzwerke würde auch im Spannungsverhältnis von unterschiedlichen Interessen stehen. Sicherlich haben die sozialen Netzwerke einerseits ein Interesse daran, Social Bots in ihren Netzwerken zu entdecken und die entsprechenden Konten zu sperren resp. zu isolieren, um ihr Geschäftsmodell glaubwürdig anbieten zu können. Vermehren sich Social Bots überproportional, könnte sich dies negativ auf die Plattform auswirken, da die Nutzer keinen Sinn mehr darin sehen, auf einer Plattform zu kommunizieren, auf der sich zum grossen Teil nur noch Social Bots als Gesprächspartner befinden. Andererseits kann sich ein zu transparentes Vorgehen gegen Social Bots und dessen Offenlegung negativ auf die potentiellen Werbekunden auswirken, da diese ihre Anzeigen selbstverständlich möglichst effektiv bei realen Nutzern platzieren möchten. Die Unternehmen haben denn auch kein Interesse daran, Zahlen zu ihren bereits stattfindenden Aktionen gegen Social Bots öffentlich zu machen. Jüngst bestätigte jedoch Twitter, rund 150'000 Konten gesperrt zu haben.[69] Vor diesem Hintergrund ist es fraglich, ob allein mit Instrumenten der Selbstregulierung auf die Risiken von Social Bots für die freie Meinungsbildung reagiert werden kann.

2. Medien

Medienschaffende stellen zentrale Akteure in der demokratischen Meinungsbildung dar. Viele Medienschaffende sind selber in den sozialen Netzwerken aktiv oder nutzen diese als Quelle von Informationen oder Trends.[70] Durch Medienschaffende können daher unter Umständen die Auswirkungen von Social Bots verstärkt werden. Die Selbstregulierung der Medienschaffenden in der Schweiz erfolgt durch den *Schweizer Presserat,* der dem Publikum und den Medienschaffenden als Beschwerdeinstanz für medienethische Fragen zur Verfügung steht.[71] Der Presserat soll mit seiner Tätigkeit zur Reflexion über grundsätzliche medienethische Probleme beitragen und damit medienethische Diskussionen in den Redaktionen und im Publikum anregen. Der Schweizer Presserat nimmt auf Beschwerde hin oder von sich aus Stellung zu Fragen der Berufsethik der Journalistinnen und Journalisten. Grundlage der Stellungnahmen des Schweizer Presserats bilden dabei die «Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten»[72] (einschliesslich der im Zusammenhang mit der Erweiterung der Trägerschaft des Presserats auf Verleger und RTV-Veranstalter vereinbarten Protokollerklärungen), die dazu vom Schweizer Presserat erlassenen Richtlinien sowie die Praxis des Schweizer Presserats. Die Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten ist sehr allgemein gefasst, jedoch umfasst sie auch die Verpflichtung, nur Informationen, Dokumente, Bilder und Töne zu veröffentlichen, deren Quellen ihnen bekannt sind. Sie dürfen keine wichtigen Elemente von Informationen unterschlagen und weder Tatsachen, Dokumente, Bilder und Töne

---

64 Zum Begriff vgl. Ruch (FN 55), 419 ff.; Hettich (FN 55), N 513; Errass (FN 55), 87 f.; Christoph Errass, Kooperative Rechtssetzung, Zürich/St. Gallen 2010, 46 ff.

65 Vgl. beispielsweise die Twitter-Regeln, Internet: http://twitter.com/rules, oder die Erklärung der Rechte und Pflichten von Facebook, Internet: https://de-de.facebook.com/legal/terms; ferner mit Bezug auf die künstliche Steigerung von Videoansichten, YouTube Community Guidelines, Internet: https://support.google.com/youtube/answer/2801973.

66 Vgl. Ziff 3.2 der Erklärung der Rechte und Pflichten von Facebook (FN 65): «Du wirst mittels automatisierter Mechanismen (wie Bots, Roboter, Spider oder Scraper) keine Inhalte oder Informationen von Nutzern erfassen oder auf andere Art auf Facebook zugreifen, sofern du nicht unsere vorherige Erlaubnis dazu erhalten hast.» Vgl. dazu auch Martin Eckert, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, 265–273, 272.

67 Vgl. Abby Ohlheiser, Mark Zuckerberg outlines Facebook's ideas to battle fake news, The Washington Post, 19.11.2016, Internet: http://wpo.st/cqhJ2.

68 Vgl. Mark Zuckerberg, Facebook Post, 18.11.2016, Internet: https://www.facebook.com/zuck/posts/10103269806149061.

69 Meier/Wilton (FN 14).

70 Vgl. Markus Prazeller/David Hug, Twitter und Persönlichkeitsschutz, Jusletter vom 24.10.2016, N 1.

71 Vgl. dazu Art. 1 des Geschäftsreglements des Schweizer Presserats, Internet: http://presserat.ch/Documents/Geschaeftsreglement 2015.pdf. Allgemein dazu vgl. Peter Nobel/Rolf H. Weber, Medienrecht, Zürich 2007, 329 ff. International hat sich als Reaktion auf die Verbreitung von Falschinformationen das Netzwerk First Draft News gebildet, Internet: https://de.firstdraftnews.com.

72 Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten, Internet: http://www.presserat.ch/Documents/Erklaerung 2008.pdf.

noch von anderen geäusserte Meinungen entstellen. Sie haben unbestätigte Meldungen, Bild- und Tonmontagen ausdrücklich als solche zu bezeichnen. Die Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten und die darin konkretisierte Wahrheitspflicht bieten daher durchaus Ansatzpunkte, um von Medienschaffenden eine besondere Aufmerksamkeit zu verlangen, wenn sie sich in ihrer Arbeit auf Informationen aus sozialen Netzwerken stützen oder anhand von sozialen Medien gewisse Trends thematisieren.[73]

D. Verhaltensgebote

Sind die bestehenden Informationspflichten nicht ausreichend und bestehen keine selbstregulierenden Standards von privater Seite oder sind diese zur Risikobewältigung nicht effektiv genug, so hat der Staat im öffentlichen Interesse und in Umsetzung seiner Schutzpflicht für die politischen Rechte der Stimmberechtigten *zusätzlich rechtliche Massnahmen* zu ergreifen.[74] Solche zusätzlichen Massnahmen müssten sich auf eine noch zu erlassende gesetzliche Grundlage stützen und haben insbesondere auch die in Art. 36 BV verankerten Anforderungen an eine staatliche Einschränkung der Grundrechte zu erfüllen. Im Vordergrund steht dabei die Prüfung der Vereinbarkeit mit der in Art. 27 BV garantierten Wirtschaftsfreiheit, da Regulierungsmassnahmen aufgrund der erheblichen Schwierigkeiten, die direkten Anwender von Social Bots zu identifizieren, regelmässig bei den risikoverursachenden Unternehmen ansetzen müssten.[75]

Bei der Diskussion von zusätzlichen staatlichen Massnahmen hat sich der Gesetzgeber vom *Verhältnismässigkeitsprinzip* leiten zu lassen. Ein schlichtes Verbot von Social Bots kommt daher mit Blick auf die ungewissen Schadens- und Wirkungsverläufe nicht in Betracht.[76] Der Staat kann jedoch zur Regulierung von Risiken unter anderem auf Verhaltensgebote zurückgreifen. Verhaltensgebote sind in der Risikovorsorge häufig anzutreffen und regeln das Verhalten einzelner Risikoverursacher direkt mit Standards, an denen sich die Befolgung einer Regel durch den Risikoverursacher messen lässt. Begleitet werden Verhaltensgebote von Sanktionen für den Fall der Nichtbefolgung und von Massnahmen zur Überwachung der Regelbefolgung.[77] Zu den Verhaltensgeboten zählen auch *Pflichten zur Selbstkontrolle*.[78] Die Pflicht zur Selbstkontrolle verlagert die Erfüllung des Regulierungsziels auf das regulierte Unternehmen, weil das Risiko nicht vollständig bekannt oder die riskante Tätigkeit aufgrund ihrer Komplexität nicht abstrakt normierbar ist. Verhaltensgebote stellen auch *Informationspflichten* des regulierten Unternehmens dar, die ein Informationsgefälle zwischen dem Unternehmen und den Kunden ausgleichen sollen und beispielsweise in Form von Warnhinweisen oder auch Kennzeichnungen erfolgen. Weiter gehören Auskunfts- und Mitwirkungspflichten gegenüber Behörden zu den Verhaltensgeboten der regulierten Unternehmen.

Verhaltensgebote in Bezug auf den Umgang mit Social Bots in den sozialen Netzwerken müssten sich jedoch alle auf generell-abstrakte Normen stützen, die auf dem Weg der Gesetzgebung noch zu erlassen wären.[79] In diesem Zusammenhang bleibt darauf hinzuweisen, dass das Regulierungsziel bei Risiken in hohem Masse unbestimmt bleibt. Im formellen Gesetzgebungsprozess hätte man sich daher auf weitgehend *allgemeine Zielvorgaben* einer Selbstkontrolle zu beschränken, z.B. dass die sozialen Netzwerke verpflichtet wären, mit einer Selbstkontrolle sicherzustellen, dass Missbräuche durch Social Bots zu verhindern seien. Diese Selbstkontrolle wäre dem jeweiligen Stand der Technik entsprechend kontinuierlich anzupassen. Mit diesem Verweis könnte eine gewisse Flexibilität gewährleistet werden, die mit Blick auf die fortlaufende Weiterentwicklung von Social Bots notwendig erscheint. Neben einer Pflicht zur Selbstkontrolle könnten die sozialen Netzwerke verpflichtet werden, ihre Kundinnen und Kunden über das Ausmass entdeckter und

---

73 Zu den rechtlichen Vorgaben im Bereich audiovisueller Medien vgl. Art. 93 Abs. 2 BV, nach dem Radio und Fernsehen unter anderem zur Bildung und zur freien Meinungsbildung beitragen, Ereignisse sachgerecht darstellen und die Vielfalt der Ansichten angemessen zum Ausdruck bringen. Vgl. auch die inhaltlichen Grundsätze in Art. 4 ff. des Bundesgesetzes vom 24. März 2006 über Radio und Fernsehen (RTVG; SR 784.40).

74 Vgl. dazu auch Isabelle Jacobi, «Die Anreize für eine Selbstregulierung sind zu gering» [Interview mit Prof. Manuel Puppis], SRF vom 28.11.2016, Internet: http://www.srf.ch/news/international/die-anreize-fuer-eine-selbstregulierung-sind-zu-gering.

75 Vgl. dazu Hegelich (FN 6), 7.

76 Allgemein dazu Errass (FN 55), 77. Zudem wäre ein Verbot auch unpraktikabel. Ein solches könnte sich lediglich gegen die Betreiber von Social Bots oder gegen die sozialen Netzwerke selbst richten. Erstere sind jedoch praktisch nicht zu eruieren, für letztere sind die Social Bots nur sehr schwierig zu erkennen (vgl. oben II.).

77 René A. Rhinow/Gerhard Schmid/Giovanni Biaggini/Felix Uhlmann, Öffentliches Wirtschaftsrecht, 2. A., Basel 2011, § 16 N 14, N 6; Hettich (FN 55), N 272.

78 Für Beispiele vgl. Errass (FN 55), 87.

79 Der Bund kann sich dazu auf seine Kompetenz zum Erlass von Vorschriften über die Ausübung der privatwirtschaftlichen Erwerbstätigkeit (Art. 95 Abs. 1 BV) stützen oder aber, soweit es sich um öffentliche Kommunikation im Online-Bereich handelt, allenfalls auf Art. 93 Abs. 1 BV. Vgl. dazu eingehend Martin Dummermuth, Die Zuständigkeit des Bundes im Bereich der elektronischen Medien nach Art. 93 BV, ZBl 2016, 335–368.

gesperrter Konten von Social Bots geeignet zu informieren oder aber ganz allgemein Beiträge von Social Bots zu kennzeichnen, soweit diese als solche identifiziert werden können.[80] Mit diesen Informationspflichten könnte wiederum eine Sensibilisierung der Nutzenden erreicht werden. Darüber hinaus könnten die Unternehmen verpflichtet werden, den staatlichen Behörden Auskunft über ihre Kontrolltätigkeit zu erstatten, damit das für die Regulierung notwendige Steuerungswissen erhoben werden kann. Mit den gestützt auf eine Auskunftspflicht generierten Daten kann der Staat besser abschätzen, ob es weitere Verhaltensgebote braucht oder ob die bestehenden Regeln angepasst werden müssen.[81] Die Risikoregulierung würde damit anpassungsfähig bleiben und wäre so ausgestaltet, dass sie neues Wissen für eine Anpassung der Regulierung generiert. Die entsprechenden Daten und eine Mitwirkungspflicht der regulierten Unternehmen würden auch den Gerichten als Grundlage bei allfälligen Beschwerden zur Entscheidfindung dienen.

V. Fazit

Die Digitalisierung und der damit zusammenhängende Wandel in der Kommunikationstechnik eröffnet zum einen neue Optionen, Demokratie zu leben.[82] Die neuen Kommunikationsformen, die sich mit der technischen Entwicklung des Internets verbinden, können zur verstärkten Diskussion von politischen Anliegen in breiteren Bevölkerungsschichten beitragen. Zum anderen dürfen die Herausforderungen und Risiken der neuen Kommunikationsformen nicht ignoriert werden. Social Bots tragen das Potential in sich, die freie Meinungsbildung zu beeinflussen. Vor diesem Hintergrund hat der Staat aufgrund seiner grundrechtlichen Schutzpflichten für die politischen Rechte zunächst bestehende Informationspflichten für die Sensibilisierung der Stimmberechtigten zu nutzen.[83] Im Rahmen einer kontinuierlichen Beobachtung des Phänomens sollte sodann untersucht werden, ob diese Massnahmen zusammen mit den Instrumenten der Selbstregulierung der Akteure im demokratischen Meinungsbildungsprozess genügen oder zusätzlich staatliche Regulierungsmassnahmen ergriffen werden sollten. Diese müssten mit Blick auf die ungewissen Schadens- und Wirkungsverläufe von Social Bots und unter Berücksichtigung aller involvierten öffentlichen und privaten Interessen diskutiert und flexibel ausgestaltet werden.

---

80 Das soziale Netzwerk «Slack» (https://slack.com/) kennzeichnet beispielsweise alle Nachrichten, welche über die automatisierte Programmierschnittstelle (API) veröffentlicht wurden (vgl. Georgi [FN 5]). Damit werden jedoch nicht nur Nachrichten von Social Bots, sondern alle Arten von programmierten und automatisierten Nachrichten gekennzeichnet, weswegen die Gefahr besteht, dass die Kennzeichnung einen Teil ihrer Wirkung verliert.

81 Zur Notwendigkeit der Flexibilität vgl. Ruch (FN 55), 410; darüber hinaus sind Massnahmen des Bundes von Verfassung wegen auf ihre Wirksamkeit hin zu überprüfen (Art. 170 BV).

82 Vgl. dazu auch Jens Kersten, IT und Demokratie, in: Wolfgang Hoffmann-Riem (Hrsg.), Innovationen im Recht, Baden-Baden 2016, 303–336, 306.

83 Allgemein zur Forderung von Massnahmen zur Förderung der Mündigkeit der Bürger in der digitalen Welt vgl. Helbing et al. (FN 5).