Manipulation in Social Media

In brief

- So-called “social bots” can create and send automated messages, thus potentially influencing political and other decisions.
- Based on the data collected, messages can be tailored to personal preferences and address small groups or individuals.
- Laws are required to describe when and to what extent social media operators need to restrict activities of social bots.

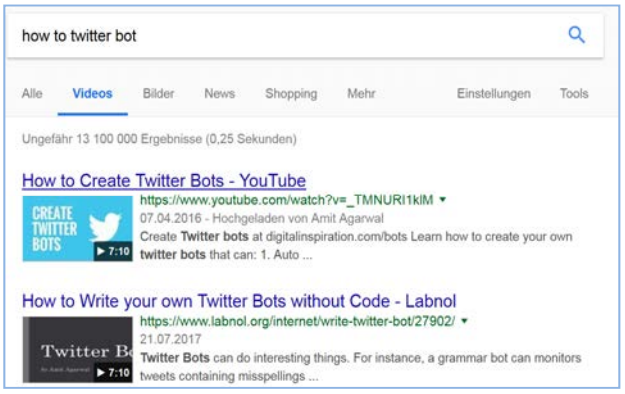
What is it about?

“Social bots” are programmes for the automated distribution of content in social media, which can be used to manipulate behaviour and opinions. Over the past several years, social bots, “microtargeting” and “dark posts”, i.e. the targeted addressing of individuals or small groups, have increasingly been used in both politics as well as the economy to, for example, influence electoral and consumer behaviour. Widespread use has the potential to considerably hamper free formation of opinion and harm democracy.

Social bots are algorithms used to influence the opinion of users of social media platforms. Bots can produce sufficiently meaningful texts by referring to content from the Internet and mimic human-like communication. They can thus distort the content of political discussions or spread fake news to a large extent and in a targeted way. As to whether they can have far-reaching influence on electoral behaviour is currently a matter of contention. Nevertheless, it has already been proven that campaign teams have deployed bots on several occasions in European and non-European countries, especially during elections with expected narrow majorities in order to topple decisions in favour of one party.

Depending on their complexity, bots are easy to programme even for lay persons, with numerous instructions to be found on the Internet. Because of rapid progress in the fields of artificial intelligence, machine learning and big data, social bots are advancing rapidly. Their messages are therefore becoming increasingly difficult to distinguish from human ones.

Bots are often used for **microtargeting** purposes. Here, companies use large, aggregated data sets (big data) to create specific profiles to find out how to better reach consumers and how to keep track of changing consumer preferences. At the same time, however, such data is also used in politics. Addresses and movement profiles make it possible for political parties to find out where their target audience is most frequently represented. This information is then used to reach their voters in a more targeted manner. Certain personal data such as credit card bills, mobile phone plans and favourite movies allow for tailored or personalised adverts. Only a few likes on Facebook or Instagram are sufficient and meaningful enough to determine party affinity or certain personality traits with a high level of probability.



Building bots, even without coding skills.

Dark posts are news in social media, which are only visible to users of a certain target group. Platforms offer this option to anyone who pays for this service. For example, a political party can specifically show a pregnant woman those aspects of their election programme which would have a positive effect on the future life of her child. This method of microtargeting was used by some parties in the 2017 elections of the Austrian National Council. Here, intentional manipulation and a lack of transparency are problematic. It is unclear what type of and how much advertising was actually sent out during a party's election campaign. Furthermore, the main principles of an electoral programme are not made clear since only one topic is highlighted. In addition, fake news are also published as dark posts and often remain unrecognised as false reports without public control.

Application and outcome

One of several electoral campaign strategies aims at reducing the visibility of the opposition party's content by drowning it with hashtags: the more hashtags are attached to a tweet, the more widely it is distributed so that other contributions are no longer among the top results. At the same time, large numbers of followers can be generated artificially by just simply purchasing them. These followers are often bot accounts or users who trade their "follow" for a "follow back". As a result, contributions from accounts with many followers become more credible. The content of bot posts is often fairly crude, in many cases they are used to send insults, discredit and false reports about political personalities.

The extent of efforts towards targeted manipulation of opinion in social media, especially by extreme right-wing movements in German-speaking countries, is alarming. Extremist material is shared on platforms and can then be used by various actors and groups in various social networks.

During the Ukrainian crisis in 2014, a large rise in the number of bot tweets was observed, confirming the rumour that the USA had shut down a plane with 298 people on board. A study examining 1.3 million Twitter accounts found that 45 percent, i.e. 585,000 of all politically-active Twitter profiles in Russia, were bots.

Table 1: Hashtag Use on Twitter, by Perspective on the UK Referendum

Perspective	N	%
Remain (#strongerin, #remain, #voteremain, #vote in, #bremain, #labourin, #votestay, #intogether, #labourinforbritain, #greenerin)	363,217	20
Leave (#brexit, #voteleave, #leaveeu, #takecontrol, #betteroffout, #voteout, #beleave, #brexitthemovie, #euisttheproblem, #brexitbustour)	993,176	54
Neutral (#euref, #eureferendum, #inorout, #eudebate, #june23)	475,233	26
Occurrence of All Above Hashtags	1,831,626	100

Source: Author's calculations based on Twitter sample of these hashtags June 5-12, 2016.
Note: This table reports the number of times these hashtags were used, not the number of tweets.

Source: Howard and Kollanyi 2016; https://arxiv.org/ftp/arxiv/papers/1606/1606.06356.pdf

Political manipulation by massive use of hashtags.

The two most active Twitter accounts in the Brexit debate were also bots: @ivoteleave and @ivotestay. In addition, it was possible to observe how foreign opinions influenced the debate. In general, there were many more bots on the pro-Brexit front than on the pro-EU front. The 2016 US election campaign also showed that a fifth of the users tweeting for Clinton were bots; with Trump, it was even one in three.

Besides Twitter, all other social media are also affected. Extensive dissemination of certain messages, supported by bots, is often already sufficient for their (apparent) legitimation. The (automated) manipulation of image, video and audio material is becoming easier, opening up new levels of abuse. At the same time, it is becoming harder and harder for lay persons to distinguish manipulated material from genuine one.

What to do?

If the use of social bots and microtargeting is becoming more wide-spread, free formation of opinion and thus democracy are in jeopardy. Strategies must be developed to deal with this development:

- A public, political discourse on the responsible use of social bots is necessary. Such discourse could, for example, discuss a ban on political advertising and manipulation in social media. Companies such as the operators of social media platforms could also be required to regulate the activities of social bots within specified limits (soft law). Currently, there are no policies or guidelines restricting social bots.
- All citizens – but journalists and politicians in particular – need additional digital literacy to distinguish news from trusted sources from manipulative fake news. Specifically designed training courses and guidelines would be useful for this purpose. The use of digital and social media should be learned and scrutinised as early as primary school.
- An independent body, e.g. a government agency, could be in charge of the timely correction of false reports. In addition, the use, possibilities and social impact of (automated) manipulation of opinions should be researched in more detail in order to be able to weigh up possible political strategies for action in a sound manner.

Further reading

Kind, S. *et al.* (2017) Social Bots. TA-Vorstudie, Horizon-Scanning Nr.3, Büro für Technikfolgen-Abschätzung beim deutschen Bundestag – TAB
http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Horizon-Scanning-hs003.pdf

Contact

Niklas Gudowsky

Email: tamail@oeaw.ac.at

Phone: +43(1)51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Apostelgasse 23, A-1030 Vienna; www.oeaw.ac.at/ita/en. | Frequency: The ITA Dossiers are published irregularly and publish the research results of the ITA. The ITA Dossiers are published in print in small numbers only and are made available open access to the public via the Internet portal "epub.oeaw": epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960 | This work is licensed under a Creative Commons Attribution 4.0 International License: creativecommons.org/licenses/by/4.0/ | ITA Dossier no. 38en, July 2018 | epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier038en.pdf |
Main-author: David Heckenberg