BOTS AS AGENTS OF EXPRESSION: 
Regimes of visibility and the power to create networks  

LORENA LUCAS REGATTIERI 
PhD student in the Communication and Culture Graduate Program - School of Communication Studies, UFRJ. Rio de Janeiro-RJ, Brazil. Email address: lorenaufes@gmail.com. ORCID: https://orcid.org/0000-0002-8747-1053.

Submitted on: 12 April 2019 / Reviewer A: 8/22/2019; Reviewer B: 7/17/2019; Reviewer A: 8/21/2019 / Accepted on: 22 August 2019

DOI – http://dx.doi.org/10.22409/contracampo.v38i3.28504
Abstract

What have we learned about the use of robots in social networks and their communication effects? Considering the contemporary media practices, critical algorithmic studies have been debating a transformation in the regimes of visibility (Magalhães, 2018). This article takes up a case study of the 2014 presidential elections on the use of bots on Twitter as agents of expression. When collecting digital data from Twitter, we process with a qualitative-quantitative technique of analyzing social networks to map computational propaganda strategies. Thus, under the effect of bots, the modulations produced from the interaction between human and non-human actors provide new parameters for understanding political-communicational phenomena.

Keywords
Bots; Visibility; Artificial intelligence; Social network analysis.

---

1 This article is the result of recent updates to the dissertation and new investigations carried out as part of the PhD program.
Scenario: the use of bots in the digital space

The use of bots as tools - its transformation from an agent technology into a new category of “believable agents” - demands a more attentive look with regard to what is behind the human trend to anthropomorphize things. On the one hand, attributing character and personality to software programs make them friendlier to human eyes. Seeing them as similar beings smooths the rough edges of the harsh reality of the human-computer interface. [...]. However, there is a down side. Personification overshadows an important truth about the relationship between humans and software tools. The dichotomy between “us” and “them” is false. We’re in this together. Software tools – whether we call them bots or agents, whether they are believable characters or not –are extensions of ourselves, prostheses that we use to manipulate objects outside our flesh-and-blood day-to-day life (Leonard, 1997, p. 104).

In his book *Bots: The origin of new species* (1999), Andrew Leonard describes bots as autonomous and supposedly intelligent software programs that provide a service. Leonard, a journalist and writer of technology-focused columns for Wired magazine, puts us into contact with a historic and critical narrative on the impacts of such agents in society. This book introduces essential questions for discussions in the IT and communication fields, as they define the role of Software as a Service (SaaS), communication protocols between the Internet and the software (API) and the evolutions in terms of natural language processing (NLP). The so-called chatbots have become very popular in customer service activities, recruiting processes and social media platforms. ELIZA² is deemed the first chatterbot in the history of computer science. Although the term chatbot did not exist in 1966. This term appears for the first time in 1994, coined by computer scientist Michael Mauldin. ELIZA operated by identifying words or key terms in entries in order to answer users by using the words or key terms found in pre-programmed answers. For instance, if a human tweeted or sent a message such as “I’m unable to use your bank’s checking account bank transfer services” and the bank mentioned has a bot-based customer service, keywords will be identified and processed so that he bot may answer the user through scripted messages programmed by the developer. This kind of procedure created the illusion of being heard and interacting with an actual human being, even though this process is mechanical.

This story is important to understand the developments in the world of agents, and their effects in communication and society. In this article, I seek to bring together the areas of computer science and communication science in order to better understand the operation and implications of these software services in terms of visibility regimes and subjectivation. I intend to analyze how these interactions between people and bots modulate people’s experiences and end up contaminating on-line conversation environments. Thus, I define bots as agents of expression of computational routines interacting by way of communication protocols on social media platforms, aiming at maximize and model people’s behaviors and conversations.

Literature in the computer science area provides as vast framework of methodologies used to detect spams and bots. In this article, I analyze robots on social media as algorithmic tools as well as various approaches to discuss the effects of these agents in communication spaces. The design of autonomous agents such as bots may provide us with tools to investigate the on-line propaganda model, as well as the mass forwarding of messages on other social media, such as WhatsApp. In the case of bots, several works investigated in a wide range of political and social contexts the way these information operations are planned and coordinated in order to generate confusion and disorientation in audiences. The purpose of this study is to analyze certain aspects regarding the pattern of dissemination and circulation of information by bots, especially botnets.

---

² To find out more about the history behind ELIZA, visit: https://www.analyticsindiamag.com/story-eliza-first-chatbot-developed-1966/.
Since the 1990s, studies have been dedicated to analyzing the complexity of such agents and selection mechanisms of artificial intelligences (Maes, 1990), testing and simulating performance and action assessment conditions as they adapt to new environments, creating algorithmic models that are capable of making decisions, taking into account the accelerated increase of data and the complexity of goal variations over time. These studies have provided us with a reflection on the role of agency in cognitive activities and on what is intelligence, analyzing emerging functionalities of these agents and whether these artificial intelligences are able to embody a sufficient level of intelligence in order express, capture, adapt and disseminate actions or not. These studies spearheaded by Patti Maes have revolutionized the field of artificial intelligence thanks to their approach focused on the architecture and design of autonomous agents, which have become less generalized and more realistic.

This outpouring of studies in the computer science field was appropriated by the communication studies area, especially in investigations on the use of computational propaganda in political scenarios all over the globe (Howard, Wooley & Calo, 2018; Ferrara, 2017; Wooley, Kollanyi & Howard, 2016; Howard & Kollanyi, 2016). A report issued by the Oxford Internet Institute, Computational Propaganda in Brazil: Social Bots during Elections (Arnaudo, 2017) gathered works focusing on the computer processes involved in the creation of bot accounts and in calculating the influence of such automatized processes on social media, as well as in the development of bot-detection tools (Savopoulos et al., 2018; Vosougui, S.; Roy, D.; Aral, 2018; Chakraborty et al., 2017; Silva et al., 2016; Messias et al., 2013; Benevenuto et al., 2010). In the case of the investigations carried out by LABIC (Image and Cyberculture Studies Lab), Arnaudo (2017) highlight the impact of bots in the 2014 presidential elections, the voting of the bill on the Civil Rights Framework for the Internet, the impeachment process with Vem pra Rua and the 2016 mayoral elections in Rio de Janeiro (Regattieri, 2016; Regattieri et al., 2014; Malini, 2016; Côrtes et al., 2016).

This set of studies highlights the use of bots in information ecosystems of platforms mediated by algorithms as an algorithmic tool operating amidst algorithmic cultures (Gillespie, 2017). Since then, bots, spam messages and trolls in the field of communication have been analyzed in order to understand the impacts they have as instruments for maximizing disinformation and contents with low credibility, disseminating campaigns of a political, social and cultural nature, and radicalizing and polarizing public discussions on social media. The study on the art of investigations about bots may be anchored on a platform called Botometer (Varol, 2017). This platform verifies the activity of a given Twitter account and generates a score based on how likely such account is indeed a bot. Higher scores indicate activities similar to those of bots. Therefore, the automatic process in the emulation of personal profiles on on-line social media includes a computer method for detection, estimates and characterization. The platform consists of detecting what is called social bots on Twitter, using resources extracted from public data and metadata on digital users. These include: friends, content and tone of tweets, network patterns and time series of activities. When analyzed by the platform, a given profile may be deemed a bot depending on how it behaves. However, it is possible that a human profile may be deemed a bot after being assessed by the platform. Hence, this is a case of probability, provided that the characteristics attributed as part of automation processes - as defined by the mathematical equation - indicate how often a human profile is behaving like a bot.

Bots are accounts controlled by software programs, and these accounts perform a set of automated tasks: they may post contents, interact with one another, humans and other bots through on-line connections - just as actual people. Sanger (2018); Jamieson (2018); Benkler, Farris e Roberts (2018) and Phillips & Milner (2017) discuss how the action of propaganda models on social media may be used as instruments for organization, modeling, disinformation and radicalization, capable of interfering with public opinion, in the end changing the course of election processes and debates in democracies. In the pursuit of quantitative evidence, Shao et al. (2018) analyzed the viral propagation of disinformation spread by 14 million messages sharing 400,000 articles on Twitter for 10 months, between 2016 and 2017, in the United States. The methodology used took qualitative data provided by fact-checking agencies in order to classify
parameters related to contents with high and low credibility. Thus, they found evidence that bots played a disproportionate role in the dissemination of articles taken from sources with low credibility. The results indicated that bots operated in the amplification of these contents when they were first being disseminated, before such contents became viral. At the same time, these bots operated by segmenting users with a lot of followers according to their replies and mentions. Human profiles are vulnerable to this kind of manipulation, sharing once again the contents posted by bots and starting to contribute to their formulation - with each user incorporating parts of their social network connections. Bots provide support to websites with low credibility, as they are strategically seen as the oxygen of amplification (Phillips, 2018).

In a sort of on-line militarist policy, a cyberwar in which network propaganda models are adopted and adapted for specific purposes, the automation used to shape public debate on on-line social media employs coordinated strategies by way of bots in order to form a massive herd of opinions. As important as identifying bots controlled software programs, we must understand the impact of this war in the communication field and how these tools change the regimes of visibility (Magalhães, 2018); the contaminations in subjectivation processes and in the creation of new conversation and propaganda models (Sanger, 2018; Benkler, Faris & Roberts, 2018). And what if some do this by using privileged databases? And what if there is funding for investing in artificial intelligence and machine learning tools? What was to happen to public opinion when faced with malicious contents, conspiracy theories, rumors, fake or misleading news? (Marwick & Lewis, 2018). And more, what modulates the targets of such propaganda strategies? In these processes, the figure of cyborg profile appears. They may operate as a digital influence machine (DIM) (Nadler, Crain & Donovam, 2018), allowing for the management and maintenance of contents created to disseminate messages on social media, being characterized by “an infrastructure of data collection and targeting capacities” (Nadler, Crain e Donovam, 2018), developed by ad platforms, web publishers and other intermediaries. The operation of this machine includes a structure put together to monitor users, drive target audiences and use automated technologies that increase its reach, ultimately increasing its power of influence as well. According to these authors, three essential changes in the media landscape in the United States have provided the conditions for the consolidation of this propaganda model: the decline of professional journalism, the upscaling of financial resources directed towards political influence and the growing sophistication of target advertising with little supervision.

It may be inferred that botnets carry out an initial intervention that exposes a lot of users to low-credibility information, increasing the chances of a given message becoming viral. The consolidation of the amplification of contents and the success of this propaganda model are marked by the moment when humans join this dissemination network. These dynamics results in its specific expression effects within the universe of Twitter conversations and on-line propaganda. In this study I review a series of studies involving computer and communication studies in order to understand how digital data extracted from on-line social media can point to evidence in terms of the organization, distribution and shaping of various groups on social media.

In the next section of this study I intent to analyze the relationships the simulation of virtual reality and the ways subjective expression in digital spaces is used to achieve visibility, qualifying virtuality as a territory of ethical elaborations. The construction of a decision-making process by humans in virtual spaces considers the conditioning aspects of these algorithmic tools by considering the environment in which they are located. From the digital data generated from the 2014 presidential elections, I analyze the characteristics of bot behavior that put into actions coordinated tasks aimed at reaching specific goals, taking into account the dynamics of interactions that take place in a given environment. The process of execution and performance of specific actions, as well as the planning and deliberation processes, shines a light on the architecture and design of bots as agents of expression. Lastly, this ongoing study includes charts displayed in order to show that botnets indeed establish new communication dynamics between humans and machines.
Algorithmic tools for network propaganda: clues on the circulation of information, subjectivation and mediations of visibility

Bots, as all other creatures, belong to their environment. In this case, their environment is the Internet. The proliferation of MUDs (multiuser domains), the thousands of message boards that make up Usenet news, the practicality of the countless chat rooms on the IRC network, the inexorable circulation and transformation of the World Wide Web: only unintentionally one can say that the Internet has been consciously planned, organized or regulated. It is a very successful example of the power or alternative dissemination - limitlessly creative, limitlessly changing. [...] The multiplicity of network environments is one of the reasons why the attempt at discerning a new particular genealogy or anatomy for bots is a mission filled with dangers of a semantic and logistic nature. Bots comprise not just one new species but a complete spectrum of new species, a brand-new phylum under the digital sun (Leonard, 1997, p. 17).

On a social context, distant from a fascination for technical aspects or from stressing a catastrophic future in which machines will lead to a state of inhumanity and the loss of all ethical dimensions of life, I hereby propose to map out the relationship between humans and non-humans. Guattari (2015) attempts at reconceptualizing machines, placing them halfway between inertia and invention; on the one hand, there is their empty nature; on the other hand, they are objects of subjective individuation and collective subjectivity. In this context of robotic humanization or the humanization of robotics, bots, autonomous agents, viruses, social bots, fake profiles and satires are seen, from a human perspective, as having a soul and sometimes even a certain degree of power to organize the informational space. This study aims at demonstrating that the feedback between information levels of an affective, cognitive and informational nature is the main input used by bots when manufacturing a proto-subjectivity (Guattari, 2015), with the purpose of extending the interactions between humans and machines and establishing levels of visibility.

[...] I am not advocating that we go back to an animistic way of thinking, but nevertheless, I would propose that we attempt to consider that in the machine, and at the machinic interface, there exists something that would not quite be of the order of the soul, human or animal, anima, but of the order of a proto-subjectivity. This means that there is a function of consistency in the machine, both a relationship to itself and a relationship to alterity.20 (Guattari, 2015, p. 89).

Magalhães (2018) addresses the issue of mediation of visibility. The relationship between the way networks are designed and the simulation aspects of bots on social media gives rise to diffuse frameworks in terms of production of subjectivity. The author claims that “the normative meaning end users attribute to algorithmic decisions possess constituent ethical properties” (Magalhães, 2018, p.8). This framework organized by the coordinated actions of bot networks ought to presume the reality and the perceptions that make up the way profiles express ideas in social media. Yet, behavior alteration attempts and the worth attributed to a certain way of being ethical does not constitute the identity of a final user. The objective logic and the consequences behind the actions of a given profile cannot be explained by the normativeness embedded in an algorithm, or even a bot. Individual actions on social media may be distinguished in the aspects of algorithmic governance in a given regime of visibility; however, the ethical assessment of virtue and moral aspects may undermine an individual’s own autonomy. If an individual in contact with the algorithm is under a process of alteration, the goals, parameters and perceptions engender new visibility practices. As algorithmic tools, bot operate on their respective botnets, requiring an architecture and human interactions in order to circulate and guide new visibility practices. However, botnets do not govern either ethics or morals, failing to establish any kind of code of conduct.

The central context includes the decisions made my algorithms on behalf of final users (such as Facebook’s news feed). From the non-specialized perspective of final
users, they are a sort of social and material context created not by way of complex computer codes and digital information, but by way of a deceitfully simple interface. It is an individual’s deliberate attempt at changing himself/herself in response to what he/she speculates as being the logic behind these decisions that define an ethical subjectivation as being “algorithmic” (Magalhães, 2018, p.7).

One of the most popular ways of human-human and human-machine interaction on a digital environment is virtual reality games. At least since the 1970s on-line virtual environments have been simulating the characteristics of the physical and social world, allowing for the interaction between users in a virtual reality. The first virtual simulation game was Dungeons and Dragons. A Multi-User Dungeon or Multi-Use Dimension (MUD) is a software program that operates as a virtual platform connecting various users, allowing for written commands only. Players connect to the platform, choosing their name and gender as well as writing a small biography. According to Curtis, this multi-player environment, a virtual reality that is extensible and may be accessed by user on-line, is a virtual meeting spot featuring aspects and habits found in daily life, such as people collaborating with each other in order to develop a project collectively. Despite the artificial construction of an environment and the fact that interactions take place only through text, the sensations generated have an impact on users’ lives and are understood as social phenomenon in terms of behavior. The experimentation of a virtual reality is linked to current discussions on how long users spend on social media and the way they behave and act on this other social layer of life, not that much different from players and their experiences; in order to join Twitter, for instance, users must choose a username, an avatar and write a small biography.

MUD players typically spend their connected time socializing with each other, exploring the various rooms and other objects in the database, and adding new such objects of their own design. They vary widely in the amount of time they spend connected on each visit, ranging from only a minute to several hours; some players stay connected (and almost always idle) for days at a time, only occasionally actively participating (Curtis, 1992, p. 4).

According to Turkle (1994), within the context of a virtual habitat of multiple dimensions, a MUD, computer intelligence entities raise questions on a social dimension. These entities, which I chose to characterize as bots instead of artificial intelligences, such as the author proposes, may be created by corporate players. These bots may wander across a MUD and actively participate in a virtual environment in order to persuade other players, as bots can offer information, tell jokes, be rude and give directions to wrong places. When least expected, players may be engaging in a long conversation with a bot without even realizing that the entire interaction involved an entity programmed by another player, having been in fact created in order to appear and persuade players to follow another path. In summary, it is as if they were taking part in a Turing Test without having been informed of such. Within the context of MUD virtual realities, Turkle proposes whether bots should “announce” their artificiality or not. In the world of social media, fake profiles that perform a different version of “self” experience similar situations when interacting with other users. One may perceive that famous Twitter users, such as @Samara7Days, @HugoGloss and @DilmaBolada, feature identity facets, which, after being developed over the course of time, define the “face” of these avatars. Since they impersonate someone or create their own narrative by making up a character, they both take advantage of this popularity, which is only possible thanks to the community of users who identify with the profile in question, and end up living a large share of their real life in a virtual reality. Visibility is vital when it comes to extending the life of these profiles.

---

3 The Turing Test is a test where an interrogator (a human being) asks questions to two hidden players. One player is a human being and the other one is a machine (computer). The interrogator and the players communicate indirectly through text. The test is carried out so that the interrogator is tested to identify the players through establishing a dialog with them. Lastly, the interrogator must decide which player is the human. The computer is trained through programming to imitate a human being, making use of a logical system of alternatives. If the interrogator fails to identify which player is human, it is presumed that the machine has achieved a certain level of intellectuality.
On-line social media, as a space for the simulation of such proto-subjectivity and as an extensive platform for public and interactive discussions, allow for all kinds of noise. The creator’s creative dimension and semantic web techniques make it even harder to assess on social media if who is replying or retweeting a message is a bot or not. Twitter and Facebook share this particularity, since they are fundamentally social media networks that ascribe value to popularity and influence, which can make audiences that make use of such networks more susceptible to attacks by bots. The mechanics of bot relationships is defined by repetition, while human relationships center around variation. The perceptions (impressions and ideas) originating from sensations such as agreeableness, empathy and pleasure are all associated with passion; therefore, they are not part of the realm of rationality. Therefore, the way people make distinctions between what offends or not another person or a group of people is not the same way used by bots. The case of chatbot Tay directs us towards this issue present in communication relationships. Especially in terms of politics, since the case study used was the presidential elections, and the engagement of both Dilma and Aécio supporters implicates completely different feelings when comparing the two communities. In what way would a bot be able to interact with another profile in order to win votes? That depends on its ability to detect and identify irony, humor, oddness and other kinds of interaction. This does not mean simply classifying sentences as positive, negative or neutral (Patodkar, V., 2016; Canuto, Gonçalves, Benevenuto, 2016), but requires a skill that is outside the scope of computational logic. In fact, this the greatest challenge faced by artificial intelligences and methods of social media analysis nowadays: reassembling, on a machine, the foundations deemed necessary to differentiate various feelings and emotions.

Ferrara et al. (2016) discussed the main characteristics of what called ‘social bots’, associating them with their contexts, networks, feelings and time patterns of activity. After all, what traces and marks, that is what signature elements do bots leave on this social structure? The greatest challenge is to tell humans and bits apart, taking into account how social bots mimic human behavior and their proliferation on social media. According to the authors, social bots try to mimic human users by tapping into media and information networks in order to fill their profiles and post contents that have been previously collected at a specific point in time, most often at times when a given subject is one of the most popular trending topics. In an attempt to emulate human temporality, they post contents at a frequency that raises no suspicions to the model employed by Twitter to identify bot algorithms; this strategy is a mark of how to curate and produce contents that is typical of humans. Here we have two aspects of analysis: one dedicated to investigating methods aimed at detecting bots, and another one dedicated to developing techniques to be used to identify bots’ target users. The result indicated that bots retweet more than human, while being less often retweeted. At the same time, it has been observed that bots engage in little interaction, since they do not tweet, reply or mention other users that much. Bots usually have larger usernames and the date when the profile was created is usually very recent.

Wagner et al. (2012) take as a starting point an element that is not very common among researchers, that is: understand the behavior of users that are targeted by bots in order to find out which groups are more likely to have an automated interaction with a bot. In order to do so, the authors claim that it is necessary to predict user interactions on line in order to understand their behaviors and how they are connected, as well as investigate how users maintain long-lasting relationships on social media (Cheng et al., 2011; Estrada & Mendonza, 2014). The construction of models to identify users that are more likely to be targeted and predict susceptibility levels in terms of bot attacks must include the variable of reciprocity. In light of the behaviors displayed by users when online, when bots ‘attack’ they usually explore three affinity groups, divided into network, behavior and linguistic. In general, the results indicated that the active users who are most likely to be targeted by bots are the ones that are very communicative, constantly engaging in conversations and use more affectionate words in their interactions.

On the other hand, Freitas et al. (2015) assume that Twitter is a social media platform that is
vulnerable to attacks by bots. Twitter is a very popular platform for disseminating contents, especially URLs. Studies related to clicks on spam messages (Grier et al., 2010) contribute to identify the presence of hyperlinks directing users to malicious websites. In order to assess to what extent the algorithms implemented by Twitter are able to protect the platform against bots, researchers tested 120 bots and analyzed attributes linked to the gender on the bot profile’s bio, the level of posts made, the app used for posting and the bot’s universe of relationships. The authors confirmed the hypothesis that bots can fool the methods implemented by Twitter to identify fake users in a relatively easy way, even bots that make use of simple network infiltration mechanisms.

Other results indicated that the gender indicated in the bio has no importance in these algorithms used to identify humans and machines. The frequency with which contents are posted indicated that the higher the bot’s activity, the higher the resemblance to what Twitter’s method identifies as human-like behavior. In terms of interaction, the linguistic aspect is quantifiable, even if the language used on this platform is mostly informal and realized using only a few characters. Results indicated that human Twitter users have not been able to identify which contents were tweeted by bots. Another important element identified by the article highlighted that bots have a high level of infiltration in specific groups when they are created with the purpose of joining a community of highly connected users. In summary, this analysis is very useful because it puts together an important panorama of research efforts regarding bots and politics: the fact that the gender in the bio has little importance in the interactions between humans and machines, but other elements which mimic human actions do, such as how often contents are posted, the connection density in user groups and the bot’s popularity.

Taking into account Twitter’s relevance and the volume of information circulating on that platform that is used to develop other monitoring platforms, not only in terms of politics, but also traffic, epidemics, among others, Freitas et al. (2014) have developed a method to identify bots and understand how they behave on Twitter by analyzing their attributes in terms of language, content and user information. The analysis indicated that bots tend to tweet more messages containing URLs and hashtags, when compared to human users. In linguistic terms, bots end up adopting standardized practices, which results in a model that may be identified and detected more easily. With regard to how these agents of expression behave, bots on social media are not that ‘social’, and on Twitter they do not engage in conversations as much as human users, that is, bots do not reply or mention other users as much as humans. In his work, Miranda Filho (2014) put together a methodological structure for opinion polls based on data and information taken from social media. In order to execute the task of translating the opinions expressed on social media into data, he developed several stages as part of a process that includes the definition of the sex, social level, age, feelings and self-identification of spammer users (aka bots) and profiles associated with journalism in integration with the tool that executes the classification task. After being collected, all the information is pre-processed in order to remove diacritics, punctuation marks and stopwords (articles, prepositions and adverbs), being subsequently processed so that the following framework for analyzing opinions on social media may be implemented: first, all messages are categorized and analyzed in terms of the feelings evoked (what are they thinking? What is their opinion?); afterwards, user are categorized in terms of their behavior (can I trust this user? Is this profile real? Is this propaganda or news?) and personal attributes (Where is this user from? What is their sex? How old are they? To what social level do they belong?); lastly, a sample is formed - which includes all the data and a possible margin of error - indicating the opinion expressed by users (what are they thinking? Who will win? Who do they prefer?).

However, these efforts do not analyze the changes in communication practices and their effects on the contemporary modes of subjectivation. Computational methods collaborate to a quantitative mapping and indicate aspects associated with the quality of the relationships shaped in communication spaces. Focus is placed on the optimization results associated with the enhancement of methods and characteristics seen in bots when infiltrating social strata that feed themselves by way of a digital
environment. The transformation in the regime of visibility caused by an “algorithmic ethical subjectivation” (Magalhães, 2018) indicates the level of humanity in the normativeness of digital data. It is in this sense that this case study highlights the potential of communication to generate new knowledge and insights on the subject of the human-machine interaction and its effects on the informational ecosystem, especially in the handling of a large amount of data (Shorey, Howard, 2016).

Methodology for identifying botnets: Mapping out these agents of expression

More than determining whether a profile is an automated entity, a bot or a social bot, it is important to analyze how this profile engages on line, altering itself and the way other profiles behave, transforming policies on the circulation of information on a given social media platform. In this methodological research, data are displayed in a series of network charts or maps that describe the content amplification model during the 2014 presidential elections, focusing on the candidates from the PSDB and PT parties, their relationships to one another according to various statistical measures and the analysis of botnets (bot networks). In the methodology presented, the maps have nodes that represent Twitter user profiles; vertices and links between nodes, which characterize the relationship between the nodes, such as retweets, mentions or replies; and lastly, the map is divided into modulations in various colors to describe the spatialization of the communities that make up the network.

The size of each node indicates its relevance in relation to other nodes. On the Twitter map, the architecture is defined by the connections between users and, in this case, priority is given to how many times a given profile was replicated (input degree) and how many times a profile replicated another (output degree). The vertices, or links between the nodes, make up the architecture of the network. These connections represent the relationships between the nodes. For any given pair of users in relation to the database for the 2014 presidential elections, the bigger the number of connections between a user and another user, the closer they are connected by the modulation algorithm. The overall structure of the Twitter maps is determined by the sharing patterns of user on this social media platform in relation to the PSDB and PT candidates.

We have highlighted aspects of the modularity algorithm, since the variation of Twitter communities allows us to understand the vitality in the circulation of a given content. Modularity is one of the possible measures used to detect communities on complex networks. The goal of a modularity algorithm (Blondel et al., 2008; Fortunato, 2010) when detecting a community is to identify the network’s division into communities, so that network modularity may be optimized. Botnets operate on propaganda models in order to amplify the propagation of contents, exposing a given network to all kinds of topics with the purpose of inducing shares. In order to understand the critical role of bots in the viral dissemination of contents, Shao et al. (2018) quantitatively demonstrate the efficiency of dissemination attacks aimed at spreading malicious contents. According to the researchers, bots are “super-spreaders” of low-credibility contents (such as fake news, conspiracy theories and rumors), automatically posting URLs directing users to articles, retweeting other accounts or executing automated tasks that are more sophisticated, such as following and replying other users. However, bots’ amplification patterns suggest a trend to become more engaged at specific times in the dissemination process of popular articles. That ism bots are coordinately employed for a strategic purpose, not necessarily taking part in conversations and exchanges in all stages of a propaganda model. Results indicate that bots are more prevalent in the first few seconds after an article is published for the first time on Twitter, in comparison with later stages.

From July 6 to October 28, 2014, Federal University of Espírito Santo’s Image and Cyberculture Studies Lab (Labic/Ufes) extracted tweets with messages and images related to the presidential elections in Brazil posted on Twitter. During this time (the period when candidates are allowed to
engage in their campaigns, according to the Superior Electoral Court), approximately 12 million tweets were gathered. When working with large amounts of data, filters are essential. In this investigation, we used: definition of a set time period, number of single tweets, number of tweets a day, number or retweets, number of replies, number of mentions, total number of single users and number of original tweets. With these filters, we can also analyze indexed hashtags, single hashtags, messages containing URLs and also image and video files. The terms and hashtags collected throughout this process were #debatenaglobo, #13brasiltocomdilma, #Aecio45pelobrasil, #melhorcomdilma, #aeciopelamudança, #somostodosdilma, #votoaeciopelobr45il, #aecio45confirma, #13brasiltodocomdilma, #aecio45pelobrasil, #agoraeaecio45confirma, #desesperodaveja, #ripbrasil and #impeachment.

Table 1 - Time line of information on the database collected from Twitter’s API Search

<table>
<thead>
<tr>
<th>Date</th>
<th>Users</th>
<th>Tweets</th>
<th>Original</th>
<th>Retweets</th>
<th>Replies</th>
<th>Mentions</th>
<th>Hashtags</th>
</tr>
</thead>
<tbody>
<tr>
<td>19/10/2014</td>
<td>708</td>
<td>940</td>
<td>278</td>
<td>588</td>
<td>74</td>
<td>206</td>
<td>814</td>
</tr>
<tr>
<td>20/10/2014</td>
<td>1992</td>
<td>3945</td>
<td>1553</td>
<td>2149</td>
<td>243</td>
<td>1267</td>
<td>3484</td>
</tr>
<tr>
<td>21/10/2014</td>
<td>1255</td>
<td>2404</td>
<td>952</td>
<td>1284</td>
<td>168</td>
<td>671</td>
<td>2177</td>
</tr>
<tr>
<td>22/10/2014</td>
<td>12316</td>
<td>93906</td>
<td>18319</td>
<td>71352</td>
<td>4235</td>
<td>27471</td>
<td>81697</td>
</tr>
<tr>
<td>23/10/2014</td>
<td>30088</td>
<td>220726</td>
<td>44866</td>
<td>164822</td>
<td>11038</td>
<td>66028</td>
<td>184285</td>
</tr>
<tr>
<td>24/10/2014</td>
<td>208825</td>
<td>1237126</td>
<td>391841</td>
<td>786204</td>
<td>59081</td>
<td>243831</td>
<td>694344</td>
</tr>
<tr>
<td>25/10/2014</td>
<td>69183</td>
<td>295083</td>
<td>73089</td>
<td>207272</td>
<td>14722</td>
<td>73919</td>
<td>163493</td>
</tr>
<tr>
<td>26/10/2014</td>
<td>152146</td>
<td>403232</td>
<td>120409</td>
<td>262823</td>
<td>20000</td>
<td>83275</td>
<td>189857</td>
</tr>
<tr>
<td>27/10/2014</td>
<td>44789</td>
<td>90420</td>
<td>29498</td>
<td>56249</td>
<td>4673</td>
<td>18535</td>
<td>32228</td>
</tr>
</tbody>
</table>

Source: Twitter

On the eight days of data collection through Twitter’s API Search, we gathered a total number of 2,347,782 tweets, which means 293,473.17 tweets a day. From this database, only 41,523 tweets are geotagged (a number deemed quite high in surveys using data collected from Twitter). Of these tweets, the number of single users totaled 348,680. The number of original tweets is 680,805, which originated from 196,996 users. During the last week of the election period, we identified on this database that 371,645 users sent and received messages. The types of tweet are divided into retweets, totaling 1,552,743 (66.14%) of the dataset (226,122 senders and 59,915 recipients); tweets, totaling 680,805 (29%), and replies, totaling 114,234 (4.87%) of the dataset (38,029 senders and 32,839 recipients). The number of mentions totaled 515,203 (97,581 senders and 26,859 recipients). They are identified when user mentions are found in the middle of a tweet, unlike replies to a tweet, when the mention is found right at the beginning. The interactions during this eight-day period including ATs, MTs and RTs resulted in 2,182,180 tweets (249,899 senders and 91,664 recipients).

The interpretation of such information to generate an empirical material, ready to be processed, occurs in collaboration with computational methods for gathering and mining data. The collection of tweets posted during this period was carried out by way of a script called FORD. This tool searches for tweets featuring previously selected terms, storing them on a MongoDB database, installed on a remote server. The next step is the processing of these tweets through ‘FORD parse’, stored as comma separated value files (.csv), capable of dividing these files into three other files: an AT (when tweets begin with a @ username), MT (mentions to a @username in the middle of the tweet), and RTs (retweets as an automatic share of messages posted).

In order to start extracting the perspectives (Malini, 2016) contaminated by bots, the social media analysis process proceeds with a perspectivalist method to the investigation of RTs file. Gephi (Bastian, Heymann & Jacomy, 2009) is the tool used in lab research projects involving the extraction of a
large amount of data, as it is a comprehensive software program used to analyze and generate statistical data and visual displays. By using Gephi, I was able to generate statistical reports and visual displays by designing a chart. What happens on Twitter is then revealed by the statistical data obtained and the filters used. This free tool may generate important statistics, such as the input or output degrees, hubs and authorities, modularity, the centrality of intermediation, approximation and eigenvector. These results allow us to navigate across the trails left by bots and the semantic framework of a given network.

The second step is to apply the modularity algorithm in order to find the perspectives viewed in the core area of the software, such as network fractions in distinct colors, since we used Gephi, based on the Louvain method (Blondel et al., 2008). This method identifies communities in weighted charts, bearing characteristics such as accelerated capture heuristics, with modularity optimization. The Louvain method is an algorithm that finds high-modularity partitions on large network in a short amount of time, generating passes consisting of two phases: first, local modularity is optimized, with a random order of vertices sweeping the entire network; and second, the communities where passes are repeated in an iterative way are aggregated, until modularity is maximized and no increase is possible. Visually, the clusters or sub-charts indicate the context in which these associations between social media profiles - whether human or non-human - were formed. They agglomerate and come closer to those with whom they have a higher level of affinity. Dislike is a divisive force that indicates lower affinity. We have invested in this approach, since the modules visually present the area of interest for bot activities in network propaganda models.

The last step in order to mold a perspective is to explore Gephi’s “Data Lab” section, a chart similar to an Excel table. On this table, researchers ought to export the names indicated on each cluster, then generating a new comma-separated-value file associated with such perspective. The process continues based on this new file, which shall be called clusternames.csv, in conjunction with the initial files containing all clusters, named tweets.csv. By understating that the parts are bigger than the whole, we then isolated, with this last processing, all tweets and metadata that each cluster contains within itself. If each cluster carries out a new processing of the FORD algorithm, we will see that it is possible to generate a new framework of relational information referring to the expressions that mold each perspective. Such information may be a network of hashtags, most frequently used words, most active users and most used hashtags. The possibilities are countless in terms of metrics.

After identifying the expression scenario for each perspective, we applied weighted degree statistics in order to measure the volume of tweets and retweets. In order to analyze the influence of profiles on the network and detect anomalies in user behavior, we process these statistical data in order to visualize the nodes with a higher or lower level of tweets. The mean weighted degree takes the average sum of the weights of all edges connected to a node. This metric may indicate tactical spamming characteristics. This weighted degree provides the input and output metrics of a node, measuring the volume of messages that this node is sharing or not. Thus, bot networks may indicate tens of thousands of profiles that falsely represent real users, but are not in fact real. These accounts post, tweet and mention thousands of messages, complimenting and/or ridiculing one candidate or the other. Hence, this statistical information shows the massification and notification nature of automated users. Botnets also make use of popular hashtags and try to saturate them by posting large amounts of spam messages. These massification actions are a tactic that may be used as an attack, by deploying numerous bots to act on a specific task or even by automatically programming tweets with specific words or phrases, in addition to organizing a large group of human users on Twitter so they can post the same message simultaneously.
The hashtag chart allows us to view the groups formed by the co-occurrence of two hashtags. With the modularity statistics, we grouped hashtag communities formed by user who share those hashtags, with the purpose of accessing a certain point of view. By using input degree statistics, we have highlighted the hashtags mostly used by users (as it may be seen on the chart). In blue, we have the group of hashtags referring to presidential candidate Aécio Neves (PSDB): #Aécio45Confirma, #agoraac3eio45confirma, #votoaeciope4lo45il, among others. On the other hand, in green, we can see the group of hashtags supporting President Dilma Rousseff (PT): #13brasiltodocomDilma, #desesperodaveja, #somostodosdilma, among others. Hashtag #DebatenaGlobo was the hashtag used by Globo TV to promote the presidential debate on social media. We see a proximity of Aécio’s network to the TV debate hashtags, while the group of hashtags in Dilma Rousseff’s support maintains a certain distance. Since we also carried out a survey the day following the run-off election (October 28, 2014), the #RIPBrasil hashtag ended up gaining a lot prominence in view of the outrage expressed by Aécio Neves (PSDB) voters and the anti-PT network.
BOTS AS AGENTS OF EXPRESSION: Regimes of visibility and the power to create networks

Chart 2 - Most shared tweets during the eight days (October 21-28) in which data on the 2014 presidential election was collected

<table>
<thead>
<tr>
<th>Tweet</th>
<th>Retweets</th>
</tr>
</thead>
<tbody>
<tr>
<td>RT @g1: Dilma chega</td>
<td>48016</td>
</tr>
<tr>
<td>RT @humdaora: no caso eu sou a dilma <a href="http://t.co/vDfdjiNqBA">http://t.co/vDfdjiNqBA</a></td>
<td>9804</td>
</tr>
<tr>
<td>RT @tittwo: fanfic: um dia antes da eleição, dilma e aécio acordam em corpos trocados. agora cada um tem 24h para convencer o brasil a não ...</td>
<td>7690</td>
</tr>
<tr>
<td>RT @Sirjoker_: MANO DO CÉU A DILMA TA MUITO MAGRA <a href="http://t.co/Q5n1KVycS">http://t.co/Q5n1KVycS</a></td>
<td>6598</td>
</tr>
<tr>
<td>RT @adamschmidel: Eu, você, dois filhos, férias em paris, mansão em miami, internet de 100 megas e 50 milhões na conta ♥</td>
<td>6327</td>
</tr>
<tr>
<td>RT @rodpocket: “o aécio sabe falar melhor que a dilma” se eu quisesse alguém que sabe falar eu votava no bial pois o video do filtro solar ...</td>
<td>5730</td>
</tr>
<tr>
<td>RT @malikdefenses: Dilma: 13 Marina: 40 Aécio: 45 CPM: 22 Ben: 10 Onze: 20 Nx: 0 Marcelo D: 2 U: 2 P: 9 Blink: 182 Brasil: 1 Alemanha: 7</td>
<td>5487</td>
</tr>
<tr>
<td>RT @barbiesemken: Tudo isso pra chegar hoje e votar na dilma...<a href="http://t.co/0UqOcsN54a">http://t.co/0UqOcsN54a</a></td>
<td>4320</td>
</tr>
<tr>
<td>RT @larrible: aecio disse que vai cuidar pessoalmente da segurança ou seja você estara dormindo e ele vai passar na rua de noite fazendo ro...</td>
<td>3896</td>
</tr>
<tr>
<td>RT @10Ronaldinho: O Brasil já mostrou que tem potencial para crescer muito mais!! Domingo vamos para as urnas mudar nosso país!! #Aecio45 #...</td>
<td>3836</td>
</tr>
</tbody>
</table>

Source: Twitter

This analysis using data on the presidential elections in 2014 in Brazil, collected in a period of eight days, aims at accessing the political game environment generated by the electoral race. The qualitative-quantitative method makes use of data and observations (both visual and written items) to build a cross-sectional study plan involving computer and communication studies. Humor and irony end up resulting in a high level of sharing. Automated behavior cannot create a tweet that is emotionally committed to this subject, but this message may be repeatedly and continually shared.

This new information generates a table showing the users that have posted the most contents during the period in question. Our investigation path included reviewing specialized literature and leads for the methodology, as well as the number of posts made in a short amount of time, indicated various automation levels in a given profile’s behavior. On the following chart, the ten most active users during the last week of the presidential campaign present various characteristics of automation, such as a high number of posts, they retweet or are retweeted very often, and have a high number of mentions with a low level of replies. Some of them are on hiatus (when a given profile has not posted any messages for a while); another one has made a lot of posts, but with little interaction; one user has no profile picture; other were only retweeted; most profiles were mentioned quite often. When analyzing these profiles, we may see an attempt at creating a personality for these users. In the automation process of these users (activism, remunerated marketing, bots, voter fans, and “rented” profiles), we can see that these profiles show an expressive visual and lexical engagement in the presidential race.
With the visual charts and the metrics on profile behavior we are able to map out network pulses.

In practical terms, these statistic metrics and a qualitative analysis of the tweets equalize the quantitative-qualitative methodology of the survey with social data. The topological and time context of the signs of these coordinated effects on the chart indicate the strategic mode of action of botnets. The most active users serve as anchor profiles for our analysis, but not alone. Bot networks - as seen in computer science studies - operate in loco in order to maximize and ramp up some hashtags. An interesting metaphor would be to image botnets being used the same fashion athletes use performance-enhancing drugs. The use of such performance-enhancing drugs may change a body’s response to a given stimulus. In general, doping cases reveal that athletes making use of these substances in a competition intend to maximize their stamina, strength, agility or even optimize weight loss. The relationship between retweeting statistics, most active users and modularity depend on the contextualization of the event or the reason behind a given stimulus. In the 2014 presidential elections, the campaigns of both candidates strategically used botnets in order to ramp up the use of the #Aecio45PeloBrasil and #SomosTodosDilma hashtag in order to maximize the cascading of information among their followers during debates and on the last days before the election. However, that does not mean - as we know from athletes who fail anti-doping tests - that the performance or the circulation of interactions is solely the products of automated accounts. Or that the path taken by those conversations is guided from beginning to end by bot networks. Bots as agents of expression operate a cascading and automated contamination strategy, with the power to create networks of interaction with humans. When used on on-line platforms of interaction, the main goal is to maximize and model the behavior of interactions between conversations and people within a given period.

Final considerations: Bots as agents of expression

Despite recognizing social media platforms as an extensive layer of a democratic and public arena for conversations, studies originating from the computer science field prioritize the development of methods that demonstrate the vulnerability of social media websites, that is, how susceptible they are to the pervasive presence of bots and their attacks. Studies in the field of ethics in information and artificial intelligence (Floridi, 2019; Durante, 2019) point to the need to continue the exploration of approaches that take into account agents of information and their respective accountability, proposing models of algorithms aimed at detecting automated activities and their gradual effects on a complex system in

---

**Chart 3 - Ten most active users during the period ranging from October 21-27, 2014. The 'Tweets' column contains the posts made by these users, from highest to lowest number of tweets**

<table>
<thead>
<tr>
<th>Profile</th>
<th>Tweets</th>
<th>Has retweeted</th>
<th>Has been retweeted</th>
<th>Has replied</th>
<th>Has been replied</th>
<th>Has mentioned</th>
<th>Has been mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>raynnierem</td>
<td>3308</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>dairosoares</td>
<td>2471</td>
<td>165</td>
<td>2362</td>
<td>6</td>
<td>14</td>
<td>80</td>
<td>1100</td>
</tr>
<tr>
<td>letrin45</td>
<td>2424</td>
<td>162</td>
<td>2213</td>
<td>17</td>
<td>142</td>
<td>48</td>
<td>616</td>
</tr>
<tr>
<td>fmmoreira66</td>
<td>2412</td>
<td>0</td>
<td>2401</td>
<td>5</td>
<td>10</td>
<td>96</td>
<td>860</td>
</tr>
<tr>
<td>artur_jaru</td>
<td>2364</td>
<td>1</td>
<td>2354</td>
<td>3</td>
<td>7</td>
<td>7</td>
<td>755</td>
</tr>
<tr>
<td>tottstu</td>
<td>2240</td>
<td>3844</td>
<td>502</td>
<td>183</td>
<td>1451</td>
<td>1338</td>
<td>2482</td>
</tr>
<tr>
<td>rfgv63</td>
<td>2195</td>
<td>0</td>
<td>2191</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>470</td>
</tr>
<tr>
<td>keunecke</td>
<td>2058</td>
<td>652</td>
<td>1958</td>
<td>20</td>
<td>3</td>
<td>167</td>
<td>722</td>
</tr>
<tr>
<td>allannsb</td>
<td>1941</td>
<td>310</td>
<td>866</td>
<td>44</td>
<td>63</td>
<td>55</td>
<td>307</td>
</tr>
<tr>
<td>aokadaokada</td>
<td>1835</td>
<td>73</td>
<td>1813</td>
<td>1</td>
<td>1</td>
<td>18</td>
<td>490</td>
</tr>
</tbody>
</table>

Source: Twitter
various areas, such as biomedicine, public administration and management services, legal frameworks and communication, of course. Taddeo and Floridi (2018) propose a translational ethical program for artificial intelligence, directed towards the formulation of prospection methodologies that may indicate risks and opportunities, aiming at avoiding unwanted consequences. In practical terms, they propose impact assessment analyses for all stages in the implementation of artificial intelligence technologies and practices, taking into account aspects such as privacy, transparency or accountability.

The 2014 presidential elections showed how the circulation of information on the Internet is relevant to the formation of a public opinion, as well as to the decisions made by voters. However, when talking about power games, the algorithm has intensified ethical discussions on to what extent a tool can structurally modulate conversations, to the point of interfering with the rules of the democratic game. The use of automated strategies - computational routines or the imitation of automated behavior - may establish another kind of truth (Beer, 2016). When analyzing Amazon.com’s recommendation technology, Bruno and Vaz (2002) have already indicated that humans and cognitive technologies share the distribution of intelligence. This agent.com is not a prosthesis of humanity and its tasks are not limited to the extension of previously-recorded cognitive functions, but include the idea of a technical object operating “with a difference, a deviation, a transformation in cognitive activity” (Bruno & Vaz, 2002, p.36). Bots as agents of expression are organized into botnets, coordinating tasks and spreading across networks according to specific and global goals. According to the scenario and the situation, bots operate by managing modularities and setting off activation patterns on the flow of information present on social media. In the future, this investigation shall intend to explore classic notions of artificial intelligence in connection with knowledge, learning, planning and adaptation in order to analyze the effects of these technologies in communication studies.

References


