FGV DAPP
DEPARTMENT OF PUBLIC POLICY ANALYSIS

BOTS, SOCIÁL NETWORKS AND POLITICS IN BRAZIL

A study on illegitimate interferences with the public debate on the web, risks to the democracy and the 2018 elections

August 20, 2017

Bots, social networks and politics in Brazil [recurso eletrônico]: a study on illegitimate interferences with the public debate on the web, risks to the democracy and the 2018 elections / Coordenação Marco Aurélio Ruediger. – Rio de Janeiro : FGV, DAPP, 2017.

Dados eletrônicos.
Inclui bibliografia.

1. Políticas públicas. 2. Eleições. 3. Redes sociais on-line. 4. Boatos (Opinião pública). 5. Internet. 6. Robôs. 7. Computação humana. I. Ruediger, Marco Aurélio, 1959- . II. Fundação Getulio Vargas. Diretoria de Análise de Políticas Públicas.

CDD – 351

CONTENTS

EXECUTIVE SUMMARY

- It is evident that social networks have the merit of sparking debates and amplifying voices in a space that allows for large repercussion.
- Several studies show how Twitter, Facebook, among other platforms, by enabling exchanges and stimulating discussions, have become important instruments of democracy.
- However, similarly to the public debate outside of the virtual world, the networks have also been used as a fertile space for the dissemination of false information.
- Automated accounts that allow for mass posting have become a potential tool for manipulating debates on social networks, especially in moments of political relevance.
- In the general strike of 2017, for example, more than 20% of the interactions that occurred on Twitter between users in favor of the strike were provoked by this type of account. During the 2014 presidential elections, the bots also generated more than 10% of the debate.
- With this, the virtual world has been allowing for the adaptation of old political strategies of slander and manipulation of political debates, now in a larger scale.
- Identifying the presence of these bots and the debates they create is fundamental for distinguishing which situations are real and which ones are manipulated in the virtual environment. Only then will it be possible to effectively understand the social processes originated in the networks.
- This research effort by FGV/DAPP issues an alert that we are not immune, and that we must seek to understand, filter and report the use and dissemination of false or manipulative information through this type of strategy and technology. It is important to be attentive and protect the democratic spaces, including on the social networks.
- In the eve of the "election year" that will define the next Brazilian president, with campaigns happening in a context of extreme competition, it is essential to map the usage patterns of these mechanisms in order to avoid illegitimate interventions on the debate, as already seen in other countries.

BOTS ON SOCIAL NETWORKS

Asleep since the demonstrations at the time of the impeachment of president Fernando Collor de Mello (1992), the streets once again became a part of Brazilian politics when the increase in bus fares caused a wave of protests in Brazil in June, 2013. In that moment, the strategy of avoiding the appropriation of the movement by the political parties - the main targets of the revolt in the streets - and the distrust in the coverage of the demonstrations by the traditional press **transformed the social networks into a recognized space for expressing the democracy,** once they became protagonists as places for organizing and spreading information.

> “The increase in the concentrated action of bots represents, then, a real threat for the public debate, representing risks to the democracy (...)”

> “When we identify bots operating for one side, however, we do not mean to say that the political and public actors situated on that side are directly responsible for the bots in their favor.”

From 2013 to today, not only were the streets occupied by partisan movements but also the **networks were flooded by old political strategies of slander and manipulation of public debates**. However, these strategies now happen in a place that allows for the rapid massification of discourses in such a way that puts at risk the credibility of the space and of the information that circulates in it. The traditional pamphleteering for parties, for example, occupies the same timeline of news spread by the press, and so do rumors and detractions propagated by political actors from the whole spectrum of political parties.

> “This research effort presented here wants to issue an alert that we are not immune and that we must be concerned with seeking to understand, filter and report the use and dissemination of false or manipulative information (...)”

The internet and the social networks have become a very important, growing, and dynamic field of the public debate and of the dispute between narratives, which lead to the pursuit of hegemonies in politics. This reality makes room for legitimate and factual discussions, but also for ill-intentioned, illegitimate and nonfactual discourses (fake news).

In addition to this fertile environment for the dissemination of opinions, the automation of publishing tools allowed for the appearance and propagation of **bots - accounts controlled by software posing as human beings, which have already dominated part of the life on social networks and actively participate in discussions during political moments of great repercussion.**

The study carried out by FGV/DAPP shows that this type of account was responsible for more than 10% of the interactions on Twitter during the presidential elections of 2014. During protests for the impeachment, these bot-provoked interactions represented more than 20% of the debate between supporters of Dilma Rousseff, who made significant use of this type of mechanism. Another example we analyzed shows that almost 20% of the interactions in the debate between users in favor of Aécio Neves during the second round of the 2014 elections was motivated by bots.

In political discussions, bots have been used for the whole spectrum of political parties not only to obtain followers, but also to conduct attacks against the opposition and forge artificial discussions. They manipulate debates, create and disseminate fake news and influence the public opinion by posting and replicating messages in a large scale. For instance, they commonly promote hashtags that gain prominence with the massification of automated posts in order to stifle spontaneous debates on a certain topic.

> We demonstrate with this effort two of DAPP's commitments. The first one is related to the monitoring of the debate on the networks and to the attention to democracy. The second one is the continuous effort to develop and improve technologies to detect and understand this phenomenon.

When we identify bots operating for one side, however, we do not mean to say that the political and public actors situated on that side are directly responsible for the bots in their favor. Several interest groups could be using this type of resource for the dissemination of information. In truth, in a broad sense, there are even bots operating abroad. This actually entices a reflection not only about internal manipulation, but also beyond the national political boundaries, suggesting the hypothesis of the existence of even more actors, strangers to the national scenario, operating these mechanisms on the networks.

The increase in the concentrated action of bots represents, then, **a real threat for the public debate, representing risks to the democracy** by manipulating the process of consensus building in the public sphere and in the selection of representatives and government agendas that can define the future of the country.

Therefore, identifying these bots becomes a challenge of great importance, since their operation in increasingly refined and capable of replicating human patterns more precisely. Distinguishing the real side with the manipulated one, in the analysis of ongoing social and political processes, is decisive both for the government - whose decision-making process must be anchored in qualified information - and for the civil society, which reverberates the agenda produced on the networks in debates and actions outside of them.

That is why **FGV/DAPP developed a refined system that generates content algorithmically for identifying suspicious accounts that act as bots,** whose results demonstrate the important role played by bots in key moments of recent Brazilian politics.

Although the bots operate in favor of specific agendas, that does not mean that they completely dominate the net or that the final perception of the majority of people will be a direct result of the influence of these devices. What we have found, however, is that they exist, they already operate on the Brazilian debate, they follow patterns and they seek to influence. Above all, this research effort presented here wants to issue an alert that we are not immune and that we must be concerned with seeking to understand, filter and report the use and dissemination of false or manipulative information through this type of strategy and technology. We must be attentive and protect the democratic spaces, including on the social networks.

Considering that the upcoming elections will have a critical importance for the country, and supposing that our case will not be so different from other democracies in recent electoral periods, where clear manipulation attempts occurred (France, United States etc), we demonstrate with this effort two of DAPP's commitments. The first one is related to the monitoring of the debate on the networks and to the attention to democracy. The second one is the continuous effort to develop and improve technologies to detect and understand this phenomenon.

The first phase of this study, presented here, was concentrated on political moments of high repercussion on the networks in the past three years: 1the elections of 2014, 2the impeachment of Dilma Rousseff, 3the municipal elections of 2016 and 4the general strike of 2017**. The analysis considered multiple characteristics and metadata that indicate the presence of suspicious accounts.**

The study of the use of bots in the period analyzed already demonstrates clearly the damaging potential of this practice for the political dispute and the public debate. One of the most evident conclusions related to this issue is the concentration of these acts in political poles located in the extreme end of the political spectrum, artificially promoting a radicalization of the debate and, consequently, undermining potential bridges for dialogue between the different existing political fields. Another glaring element is the "swelling" of political movements that are, in reality, of a much smaller dimension. When added together, **these and other risks represented by bots are more than enough to cast light on a real threat to the quality of the public debate in Brazil and, consequently, of the political and social process that will define the years to come.**

Marco Aurélio Ruediger
FGV/DAPP Director

WHAT ARE THEY AND WHAT DO THEY DO?

An important means of communication, information and construction of connections, the social networks are an increasingly significant part of our daily lives. Studies carried out by the Pew Research Center show, for example, that **the majority of adults in the United States (62%) use social networks to stay informed.** However, 64% state that the fake news circulating on the networks cause "confusion" about daily facts and events. It is in this environment of "trust" but high circulation of dubious information that bots proliferate.

At first, automated accounts may even contribute positively in certain aspects of life on the social networks. Chatbots (chats operated by bots), for example, speed up the service to clients of companies and, in some cases, even aid refugees in processing their visa requests. **However, the growing number of bots acts, in truth, with malicious intent.**

Social bots are accounts controlled by software that artificially generate content and establish interactions with non-bots. They seek to imitate human behavior and pass as humans in order to interfere with spontaneous debates and create forged discussions. With this type of manipulation, the bots create a false sensation of wide political support to a certain proposal, idea or public figure, change the course of public policies, interfere with the stock market, disseminate rumors, fake news and conspiracy theories, generate disinformation and content pollution, in addition to luring users to malicious links that steal personal data, among other risks.

At the same time, the social networks have become an integral part not only of the personal life of the citizens, but also of their political activity and of the acts of their representatives. Parties and other movements of social representation also use the space to engage voters, attack opponents and promote debates around their interests. In this case, it is common to observe **the orchestrated use of bot networks (botnets) to generate a movement at a certain moment, manipulating trending topics and the debate in general.**

These actions have been identified in important events of international politics, such as the American elections of 2010, the election of Donald Trump in 2016 and the United Kingdom European Union membership referendum, the Brexit. In Brazil, the scenario is not different: orchestrated bot actions occurred in key moments of national politics, such as the approval of the Labor Reform, the general strike of 2017, the elections of 2014, the debate about the impeachment and the municipal elections of São Paulo in 2016.

HOW CAN THEY AFFECT OUR LIVES?

When they interfere with debates developing on social networks, bots are directly striking the political and democratic processes by influencing the public opinion. Their actions can, for example, **produce an artificial opinion, or an unreal aspect of a certain opinion of public figure**, by sharing versions of a certain topic, which spread on the network as if there was, among the part of the society represented there, a very strong opinion on a certain subject (Davis et al., 2016). This happens with the coordinated sharing of a certain opinion, giving it an unreal volume and, consequently, influencing undecided users about the topic and strengthening the more radical users in the organic debate, given the frequent location of the bots in the poles of the political debate.

The automated profiles also promote misinformation with the **propagation of fake news and network polluting campaigns.** Bots frequently use social networks to reproduce fake news aiming to influence a certain opinion about a person or topic, or to pollute the debate with information that is real but irrelevant for the discussion in question. This action, which relies on the sharing of links as the main mechanism of propagation, attempts to avoid or decrease the weight of the debate about a certain subject. For this purpose, the bots generate an enormous amount of information, which reaches users at the same time as the real and relevant information, which ends up having its impact reduced. Therefore, the actions of bots not only disseminate fake news, which can have harmful effects for the society, but also actively seek to keep users from becoming adequately informed.

Another common strategy of automated profiles is sharing malicious links, aiming to steal data or personal information. This information can be used for the creation of new bot profiles with characteristics that help these bots to start connections with real users on the networks, such as profile photos. A common action that usually raises suspicions about the use of bots is an unknown user tagging someone in a shortened link with no clear identification of its content. These links, besides stealing personal information for use in the social network itself, can also direct the user to fake news or sites that will use the number of clicks to expand their influence on the network (Wang, 2010).

There have also been detections of bots aiming to manipulate the stock market. This happens when bot networks are put to work to generate conversations that involve a certain company or topic in a positive way, manipulating the network monitoring systems of the brokerage firms. This way, the shares in question could increase in value based on an optimism that was forged by the actions of bots.

A recent case of this type of action involved a bot-generated debate on the networks about the technology firm Cynk. The automated algorithms for buying and selling stocks identified this debate and started to make transactions with the company shares, whose market value increased 200 times, reaching 5 billion dollars. When stockbrokers identified that it was an orchestrated action, heavy losses had already been suffered. **This type of action shows another disruptive potential of automated profiles, this time for the economy, causing impacts that spill over to the political debates** (Ferrara et al., 2016).

This type of action suggests that the social networks, used by so many people for information purposes, could be in fact contributing for a less well-informed society, manipulating the public debate and consistently determining the directions followed by the country.

HOW DO THEY WORK?

Bots are used on social networks to propagate fake, malicious news, or to generate an artificial debate. For that purpose, they must have the largest possible number of followers. But how can an automated profile create a network around itself?

Bots spread more easily on Twitter than on Facebook for various reasons. The 140-character limit on Twitter generates a limitation of communication that facilitates the imitation of human actions. Additionally, the use of @ to tag users, even if they are not connected to your account on the network, enables bots to randomly tag real people to insert an element that is similar to human interactions.

Bots also make use of the fact that, **generally, people are not very judicious about following a profile on Twitter, and tend to act reciprocally when they get a new follower.** Experiments show that on Facebook, a platform where people tend to be a little more careful about accepting new friends, 20% of real users accept friend requests indiscriminately, and 60% always accept if they have at least one mutual friend. This way, bots add a large number of people at the same time and follow real pages of famous people, besides following and being followed by a large number of bots, in such a way that they end up creating mixed communities - which include real and fake profiles (Ferrara et al., 2016).

Some bots intend only to divert attention from a certain top and, therefore, are less concerned with their similarity to a human user than with the intensity and capability of changing the course of a debate on the networks. Other mechanisms, however, have a series of strategies to imitate human behavior and, in doing so, be recognized as such by users and detection systems.

Knowing that human behavior on the social networks has some temporal pattern in the production and consumption of content, the profiles are programmed to post according to these same rules. **Paradoxically, it is the lack of both temporal and content patterns in the long term that bots have the most difficulty in imitating, which usually allows their identification** (Brito, Salvador e Rocha, 2013). The more modern algorithms go beyond: they are capable of identifying popular profiles and following them, identifying a subject being talked about on the network and generating a short text through natural language algorithms and generating some degree of interaction.

HOW CAN THEY BE IDENTIFIED?

There is not a single characteristic that positively indicates whether a certain profile belongs to a real user or a fake, automated one. The identification is the result of the composition of multiple characteristics and interrelated indicators. Research on this field is distributed between three main lines of methods: a) through information available on the social networks themselves; b) systems based on crowdsourcing and human intelligence to identify bot profiles; and c) through machine-learning, based on the identification of certain characteristics that enable the automation of the distinction between bots and people (Ferrara et al, 2016).

There are also different hypotheses that can be used to support the search for bots on the networks. With the method that uses connections between profiles and available data on the behavior on social networks as the formula for identifying bots, some systems assume that these automated profiles will be primarily linked to similar profiles, especially in the beginning of their digital life. **That is because they need to build a base of followers to seem believable to the eyes of real users.**

This method, however, needs to be weighed against the fact that **human users are not very judicious when it comes to interactions and friendships with unknown accounts, especially on Twitter.** Because of this, after existing for some time, bot accounts will have mixed networks, not primarily composed by bots or by humans. The amount of bots among the friends of the profile, however, can be an indicator of its nature.

The crowdsourcing method starts from the assumption that the detection of bots would be simple for human beings, whose capacity of understanding and identifying their own behavior has not yet been matched by machines. A test carried out by Wang et al (2013) reached the conclusion that, in a short training mechanism for identification (showing only examples of real and fake profiles) and following the decision of the majority inside a small group of volunteers, the number of fake positive identifications was very close to zero.

This system has some difficulties. One of them is the low cost-effectiveness for networks with a lot of users, such as Twitter and Facebook. Besides that, considering that amateur evaluators do not have good performance individually - only when in a majority vote system -, it is necessary that some trained people participate to guarantee the balance of the voting system.

The detection through machine-learning happens with the coding of behavior patterns starting from the collection of metadata. This way, the system is capable of automatically identifying humans and bots based on the behavioral pattern of the profile. These systems are normally organized from a database where humans and bots have already been distinguished previously.

The user metadata is considered one of the most predictable aspects to distinguish humans and bots and can contribute to a better understanding of how the more sophisticated bots work. Identifying these bots or hacked accounts, however, is difficult for these systems. Additionally, the constant evolution of the bots makes it so that the system, built from a static database, becomes less precise over time. However, it allows for the processing of a large number of correlations and complex patterns, in addition to analyzing a large number of accounts.

The most efficient identification mechanisms combine different aspects of these approaches, exploring multiple dimensions of the behavior of the profile, such as activity and schedule pattern (Boshmaf et al., 2012). These systems take into account, for example, that real users spend more time on the network exchanging messages and visiting the content of other users, such as photos and videos, while bot accounts spend their time researching profiles and sending friendship requests.

In this sense, research shows that t**he activities of bot accounts tend to be less complex in the variety of actions they perform,** which adds another possibility to the combination of factors that allow the systems to determine for sure that a certain profile is a bot. Because this type of system combines different data, it also obtains good results from a smaller amount of information - such as the past 100 tweets -, which accelerates the analysis and processing capacity.

The studies about bot detection on social networks are inspired by the efforts for spam detection and blocking in electronic messaging systems. In this sense, there is also the analysis of shared links to identify link farms (companies that manage bots and sell likes, retweets, etc) and dynamics of interaction (Ghosh et al, 2012).

When we analyze the statistical processes that describe the interactions between users, several factors can be studied and combines to develop a model of bot detection on social networks. Some examples are:

- Variety of actions while connected to the network;
- Characteristics of the user, considering the number of friends (real people have, on average, between 100 and 1000 followers), the proportion and correlation between profiles followed and profiles that follow the user;
- Characteristics of the friendships, analyzing how users on a certain network are interacting among themselves, including patterns related to language, popularity and time in the places of interaction;
- Characteristics of the retweet network, mentions and repetition of hashtags;
- Temporal characteristics, such as average time and production of tweets;
- Content and language characteristics;
- Characteristics of the sentiment expressed through the post.

HOW IS DAPP WORKING IN ORDER TO IDENTIFY THEM?

The masses of data collected by FGV/DAPP are composed by metadata - information about the data itself - and, through this data, we explore the possibilities of identification of accounts that have acted automatically during the periods of analysis. This way, we identified that the metadata named generator refers to the platform that generates the content of the tweet, which is very useful for the detection of bots.

We decided, then, to verify all the generators used in our databases and what is the amount of tweets generated by each one of them. From these results, we verified detailed extracts about the nature of each one of them and found platforms for the automation of content production listed among the generators.

Six cases were chosen for this first analysis:

- The debate on Rede Globo on October 4, 2014 between the presidential candidates in the first round of the elections;
- The debate on Rede Globo on October 24, 2014 between candidates Dilma Rousseff and Aécio Neves, who were running for the presidency in the second round of the elections;
- The pro-impeachment demonstrations on March 13, 2016;
- The debate on Rede Globo between the São Paulo mayoral candidates on September 29, 2016;
- The general strike on April 28, 2017;
- The voting for the Labor Reform in the Senate, on July 11, 2017.

After collecting the databases related to the six cases, we verified that 1925 different generators generated the 7.8 million tweets posted about all of them. From this total, 181 produced at least 100 tweets each, and those were the ones we analyzed manually. This evaluation allowed us to identify 83 generators that produce tweets automatically in a programmed way or using the Twitter platform through automation.

CASE STUDY
2014 ELECTIONS

The run for the Presidency of the Republic in the 2014 elections was characterized by an increasingly fierce political competition, a consequence of the effervescence on the streets still fresh from the 2013 protests. On the social networks, the polarization manifested itself in an aggressive way, and part of this hostility was provoked by bots, which motivated around 11% of the discussions.

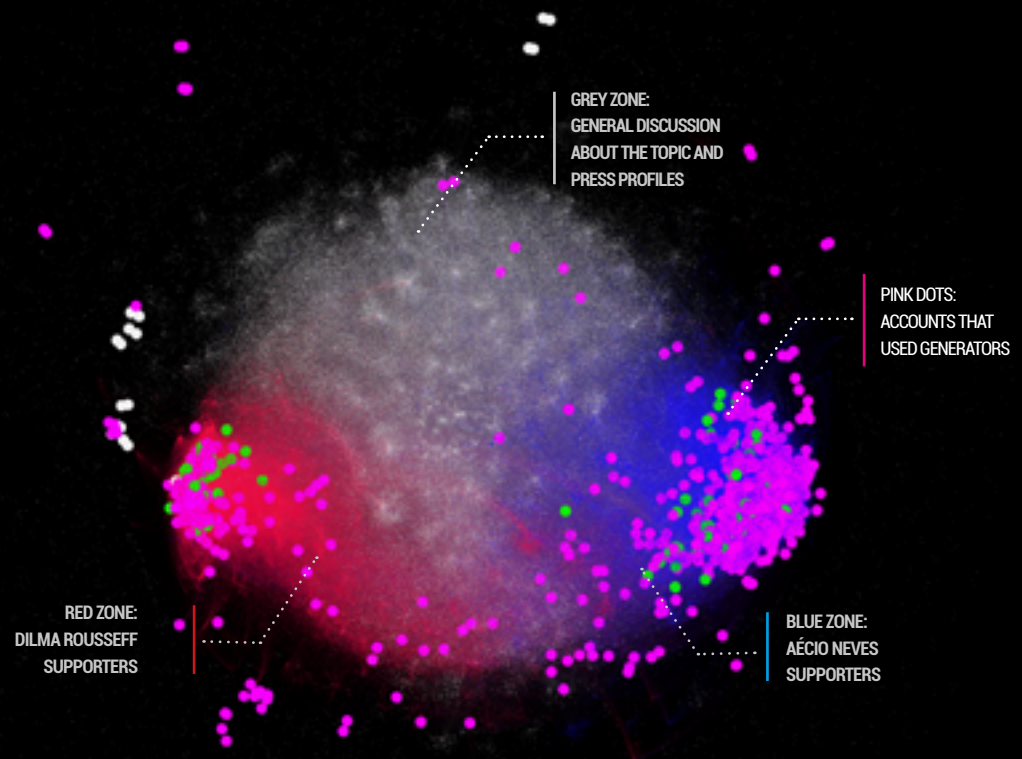
The first round of the elections was marked by the death of candidate Eduardo Campos (PSB), succeeded by Marina Silva (PSB). The dispute culminated in a deep antagonism between Dilma and Aécio (PSDB) on the second round, which resulted in the victory of then president Dilma with a narrow margin of advantage (around three percentage points).

To analyze the potential use of bots inside the discussions during the 2014 elections, we selected the tweets related to the debate between Dilma and Aécie on the second round and elaborated an interaction map from the retweets. Three major groups were identified: profiles supporting Dilma (red), profiles supporting Aécio (blue) and profiles having a general discussion about the topic - which includes press profiles (grey). We then selected the accounts that used suspicious generators and highlighted their size and color (pink).

THE DEBATE ON REDE GLOBO BETWEEN THE CANDIDATES FOR THE PRESIDENCY OF THE REPUBLIC

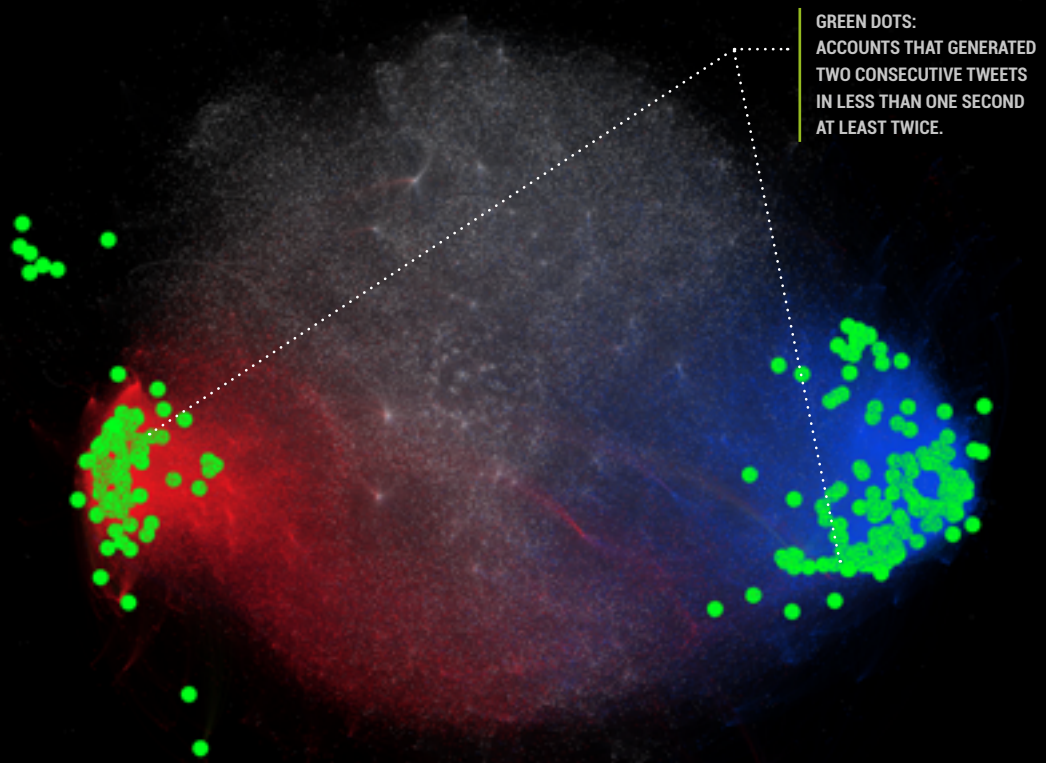
2ND ROUND
OCTOBER 24, 2014

2.307.185 Tweets
10/24/2014 00:00 - 10/25/2014 12:00



Observing the graph above, we notice that accounts that produced tweets through suspicious generators are concentrated on the extreme ends of the poles supporting the candidates. Practically none of the suspicious accounts are in the group that in general does not support any candidate (grey zone)

source: FGV/DAPP



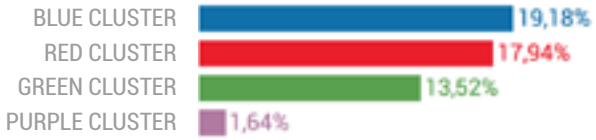
source: FGV/DAPP

From all Twitter interactions in the hours analyzed, 11.34% were motivated by tweets or retweets made by bots. Among Aécio Neves supporters (blue cluster), however, this portion of interactions with automated accounts (bots being retweeted by other bots or regular accounts) reached 19.41%. In the discussions between profiles supporting Dilma, the amount was 9.76%.

Exploring the activities of the suspicious accounts, we find that profiles are clearly automated in order to inflate the support to a certain candidate. Among these accounts, we identified the ones that posted more than once per second, an activity that raises suspicions of automation. And we highlighted in green, on the same map, the ones that produced two consecutive tweets in less than one second at least twice. Again, we notice that they are located in the extreme poles in support of each candidate.

The same can be seen in all the analyzed cases. On the following visualizations, we also colored the accounts that used suspicious generators in pink, the ones that generated two consecutive tweets in less than one second at least twice in green, and the accounts that correspond to both criteria in white.

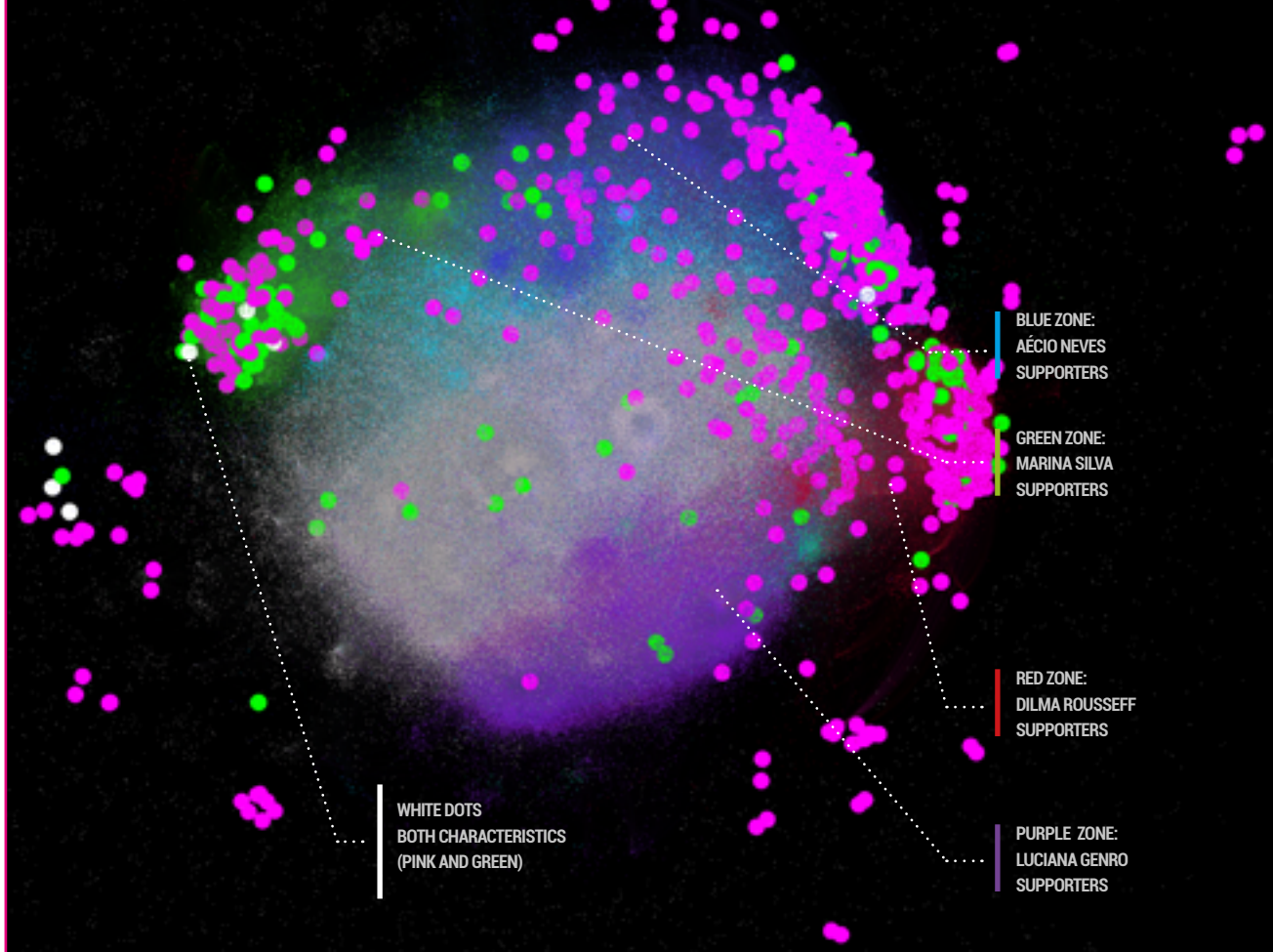
In the debate about the 1st round, the interactions with bots represented only 6.29% of the discussion on Twitter. Once again, these interactions were more significant among the profiles supporting Aécio Neves, representing 19.18% of the debate in the blue cluster. Among Dilma supporters, the amount was 17.94%.



DEBATE ON REDE GLOBO FOR THE PRESIDENTIAL ELECTIONS

1ST ROUND
OCTOBER 2, 2014

1.565.773 Tweets
10/02/2014 00:00 - 10/03/2014 12:00



source: FGV/DAPP

CASE STUDY
2015 IMPEACHMENT

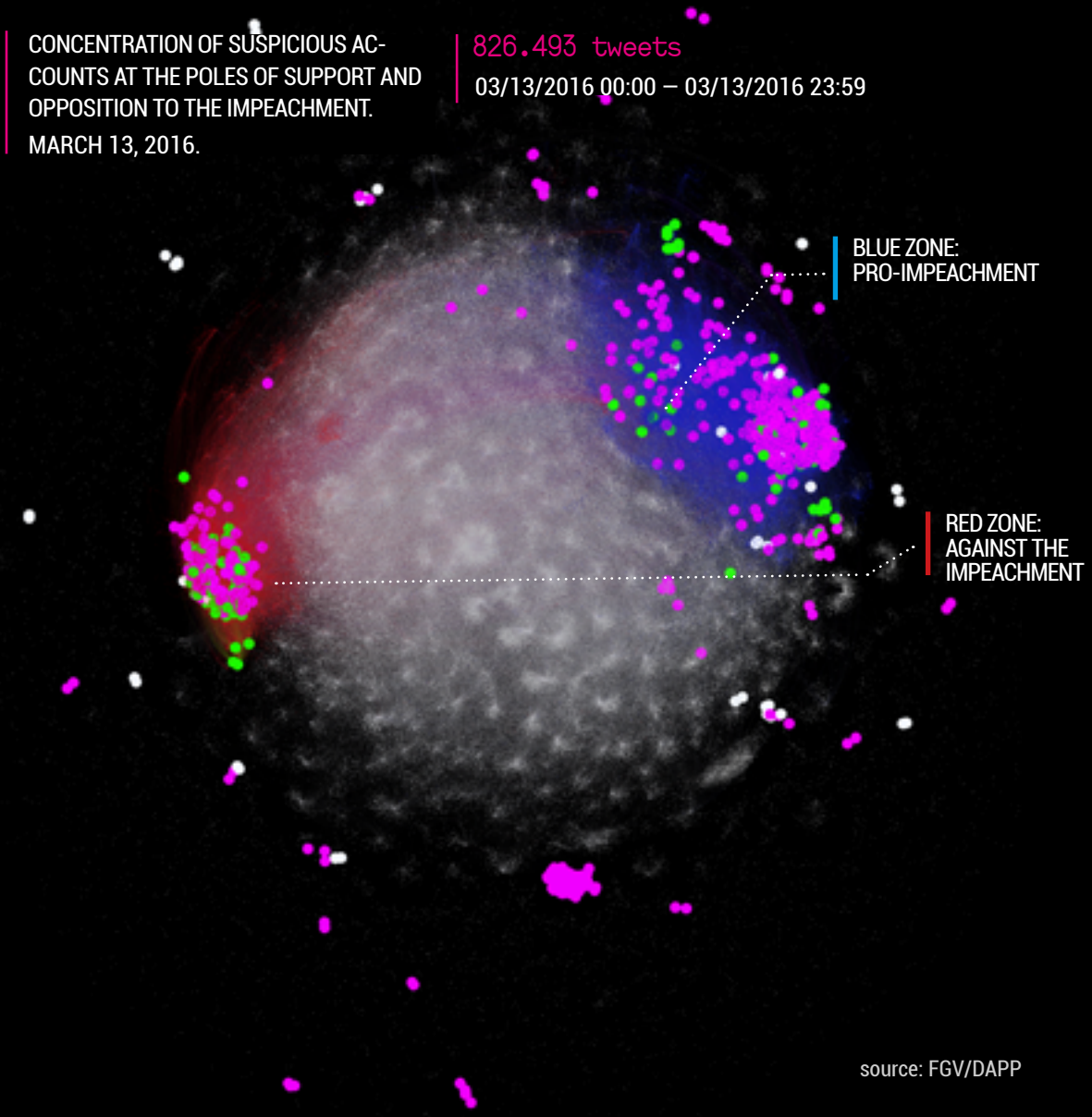
The victory of Dilma Rousseff did not halt the growing hostility between the political fields. The difficulty of the president to maintain political support in the Congress and the economic crisis in the country in recession resulted in an impeachment process with popular support manifested in a series of protests throughout the country. The graph on the right shows how the discussion on Twitter happened on the day of the largest pro-impeachment demonstration registered.

At least 10% of the interactions about the subject on this day were stimulated by bots, that is, retweets of content originated in an automated account. In the cluster of Dilma Rousseff supporters, this proportion reached 21.43%, which shows the power of influence that this type of account has on the political debate.

PRO-IMPEACHMENT DEMONSTRATIONS

CONCENTRATION OF SUSPICIOUS ACCOUNTS AT THE POLES OF SUPPORT AND OPPOSITION TO THE IMPEACHMENT.
MARCH 13, 2016.

826.493 tweets
03/13/2016 00:00 — 03/13/2016 23:59



source: FGV/DAPP

CASE STUDY
SÃO PAULO MUNICIPAL ELECTIONS - 2016

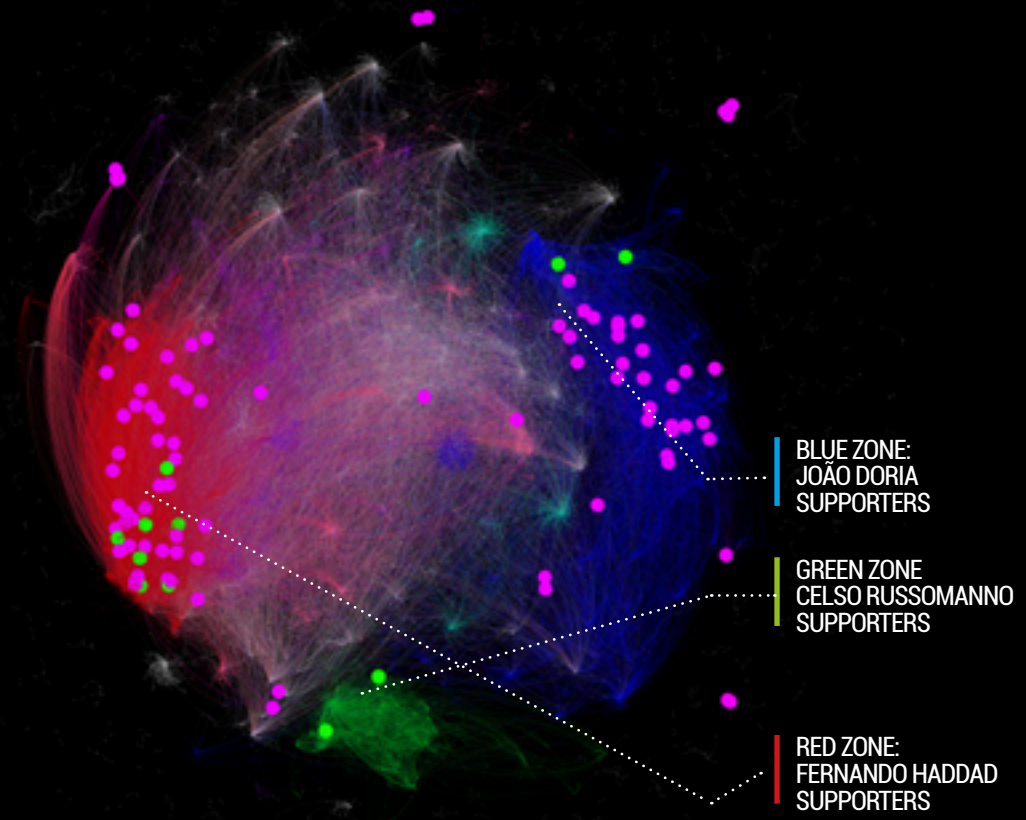
The run for the mayor office in São Paulo began with a dispersion of the voting intentions between then mayor running for reelection Fernando Haddad (PT), João Doria (PSDB), Celso Russomanno (PRB), Marta Suplicy (PMDB) and Luiza Erundina (PSOL). This divide during the first round made the electoral debates not as marked by the antagonistic discussion between PT and PSDB as the presidential elections. The election was defined in the first round, with the victory of João Doria.

The graph on the right shows how other political forces influenced the debates on the social networks. Bot-motivated interactions were also more equally distributed. Among Doria supporters, they represented 11.25% of the debate; among Haddad supporters, 11.54%; among Russomanno supporters, 8.40%.

DEBATE ON REDE GLOBO BETWEEN THE MAYORAL CANDIDATES IN SÃO PAULO

1ST ROUND
09/24/2016

148.257 tweets
09/29/2016 00:00 – 09/30/2016 12:00



source: FGV/DAPP

CASE STUDY
GENERAL STRIKE OF APRIL 28, 2017

After the impeachment of Dilma Rousseff, the debate on the legislation and labor reforms in the National Congress gained strength. The main argument in favor of the reforms was that the need for austerity to overcome the crisis should be seen as an opportunity to modernize these legislations, while the main argument against them identified in this movement a loss of rights and worsening of work conditions and of the network of social protection of the Brazilian State.

This scenario caused the labor unions and parties opposed to the reforms to convoke a general strike on April 28, 2017, counting on a large turnout to convince the political spectrum of the dissatisfaction of the people concerning these agendas. As can be observed in the graph on the right, the bots once again had a large presence. Among supporters of the strike, 22.39% of the interactions were motivated by automated tweets.

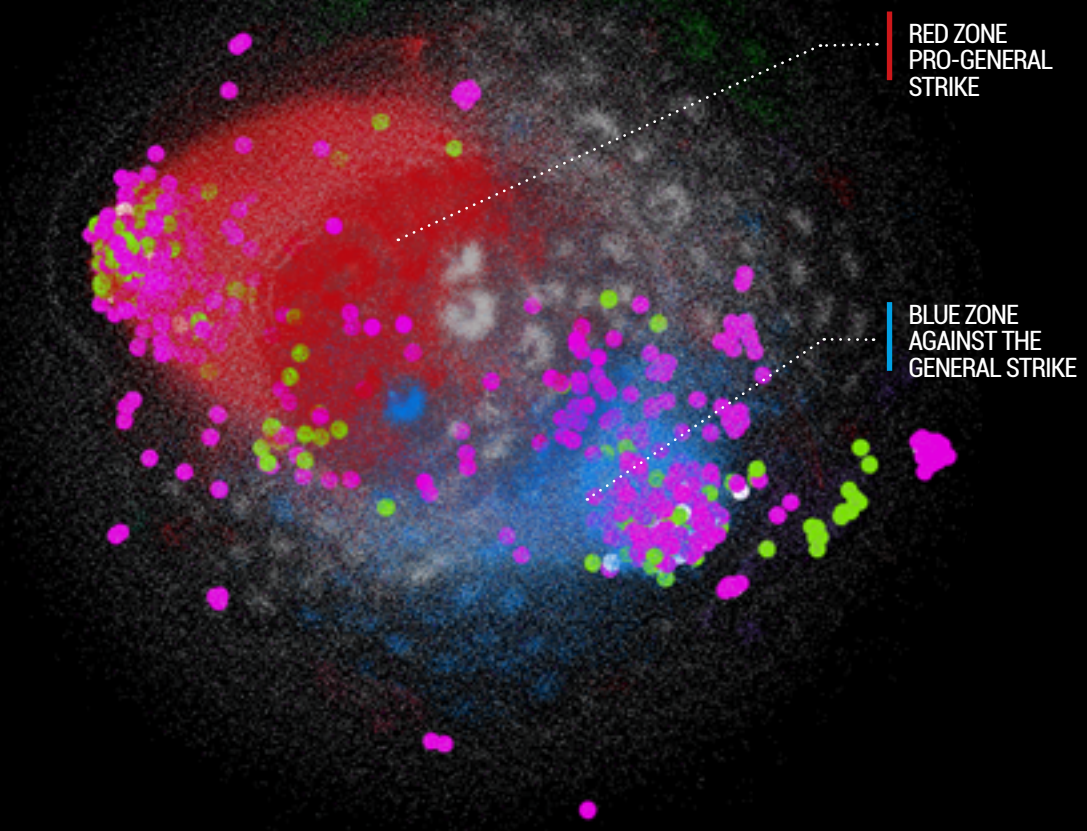
GENERAL STRIKE ON APRIL 28, 2017

SUSPICIOUS ACCOUNTS DISPERSED IN THE CLUSTER OPPOSING THE STRIKE AND CONCENTRATED IN THE CLUSTER FAVORING IT.

APRIL 28, 2017

1.460.160 tweets

03/13/2016 00:00 – 03/13/2016 23:59

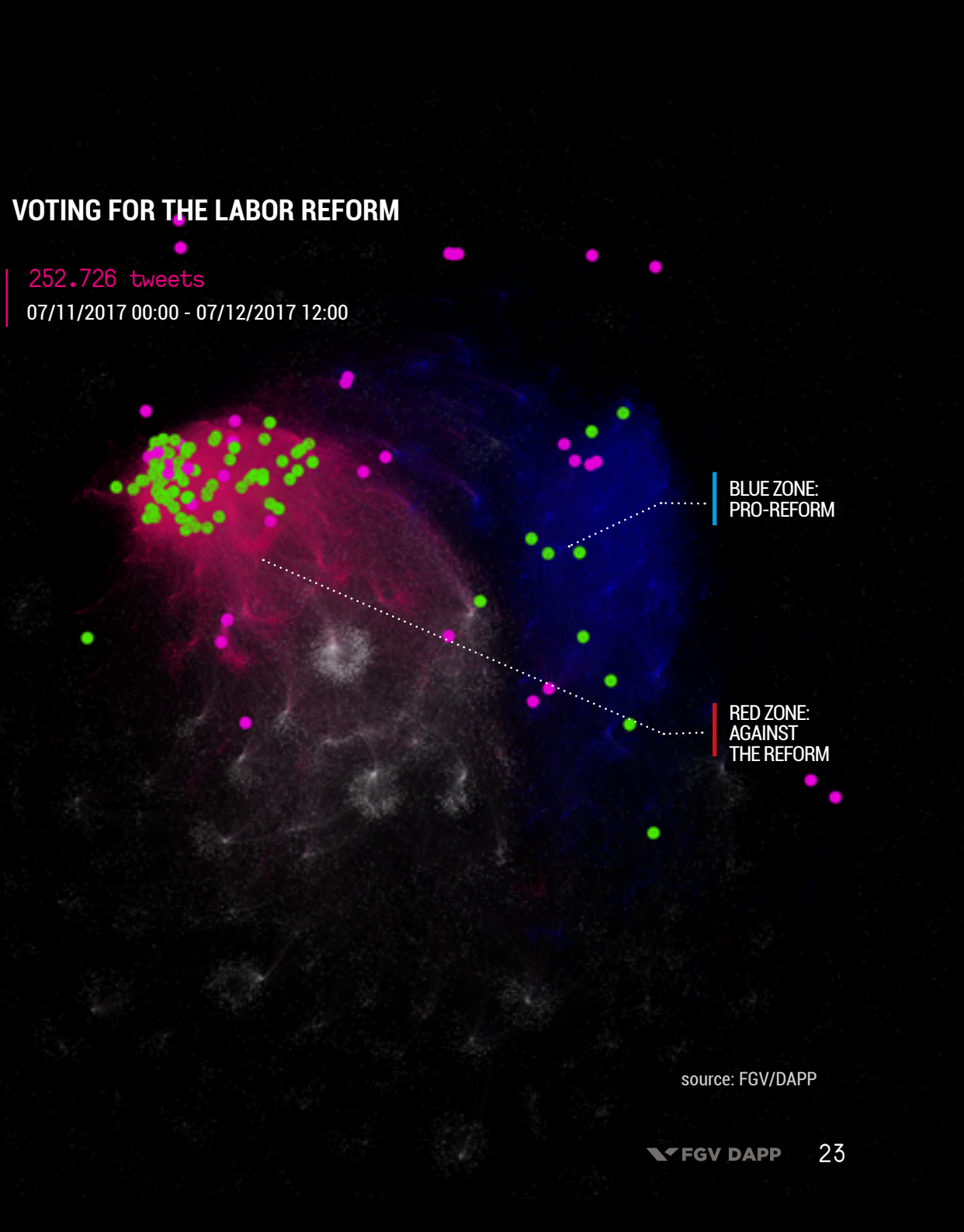


source: FGV/DAPP

CASE
VOTING FOR THE LABOR REFORM AT THE SENATE ON JULY 11, 2017

One of the main focuses of the economic recovery agenda of the current government was the approval of a reform of the labor legislation. **The debates about this proposal on the social networks followed a trend of polarization already observed in other moments of national politics.** After months of discussions, negotiations and modifications, the Labor Reform was brought to a plenary session of the Federal Senate for voting on July 11.

The bots are once again present in the two extreme ends of the debate, this time in a larger number on the pole opposing the reform. In total, we identified 2% of the interactions related to this event as automated - 3% of the interactions opposing the reform and 1% of the ones favorable to it.



VERIFICATION OF THE ANALYSIS

To validate the analysis, we manually verified a sample of 2153 suspicious accounts for the six cases chosen. This manual procedure guarantees 95% accuracy with a margin of error of 2%. **The verification sought to check whether a certain account produces content in a completely automated form.**

We observed that more than 50% of these accounts have an aspect of total automation. Approximately 9% of the accounts are institutional (from press organizations and blogs, for example), around 6% no longer exist, almost 2% were suspended by the platform, and a little over 25% are only partially automated.

As an example of the latter, there are accounts that participated of programs supporting a certain cause and authorized, in certain moments, automatic tweets to be published by their profiles on the platform. Another example are accounts that produce original content but create triggers, such as publications of news involving a certain public figure or institution, and post them in an automated form.

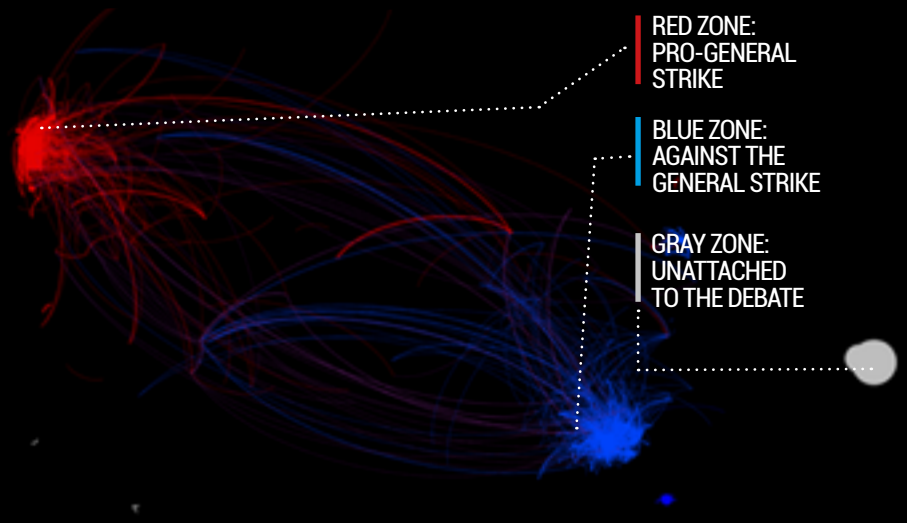
We conclude, therefore, that the verification of accounts can be contradictory and, for this moment, we consider that each tweet must be evaluated regarding its origin (whether automated or not).

We will return now to the exploration of the topography of the retweet network. Concerning the general strike, we notice that the tweets produced in an automated way served basically the extreme ends of the discussions, as seen in the graph on the right, where we filtered only the interactions conducted in tweets produced automatically.

GENERAL STRIKE ON APRIL 28, 2017

1.460.160 tweets

04/28/2017 00:00 – 04/28/2017 23:59



source: FGV/DAPP

The centers of discussion pro and against the strike participated of discussions with tweets produced automatically. The gray group consists of automated contents that use topics outside of the current debate to obtain new followers, with no apparent attempt to influence the debate.

CONCLUSION

> (...) it is indispensable to distinguish malicious bots from bots with other purposes, such as digital marketing, brand promotion, blogs and companies, institutional profiles, profiles with many administrators.

The appearance of automated accounts allowed for strategies of manipulation, dissemination of rumors and slander, commonly used in political disputes, to gain an ever larger dimension on the social networks. The significant participation of bots in the virtual environment created an urgent necessity to identify their activities and, consequently, distinguish which debates are legitimate and which ones are forged. This distinction is essential for the social processes originated on the networks to be effectively understood.

To identify bots, DAPP has been developing a methodology that combines evaluations of different metadata to encompass all the possible strategies for creating and operating automated accounts. With the ever faster dynamics of technology upgrading, bots have their activities enhanced on a daily basis, becoming closer to the human behavior. In addition, it is indispensable to distinguish malicious bots from bots with other purposes, such as digital marketing, brand promotion, blogs and companies, institutional profiles, profiles with many administrators.

Another challenge we face is the identification of cyborg accounts, those partially automated but also manipulated by humans, who post real content to create an aspect of randomness and unpredictability that is common in the human interactions. The use of these accounts makes detecting bot operation more difficult when we try to classify an account on Twitter using the binary variable of bot or human, for example.

The analysis of interactions by accounts with tweets produced automatically already indicates and confirms the use of bots in the Brazilian political debate. From the analysis carried out by DAPP of metadata that indicates their operation, we can conclude that automatically generated content has been influencing discussions on Twitter with the objective of generating advantages for political actors.

The study identified that the operation and production of automated content has not been occurring exclusively in one political pole or field. The analysis of the six cases chosen suggests that groups with different interesting, especially those located on the extreme ends of the political spectrum, become inflated and attack each other with this practice.

The analysis of the six cases chosen suggests that groups with different interesting, especially those located on the extreme ends of the political spectrum, become inflated and attack each other with this practice.

Expanding the capacity to identify and suppress the malicious automation of profiles on the social networks must be a priority. Recent analyses show that this type of action has been successful in directing the public debate, which is more and more present on the networks, directly influencing turning moments that are decisive for the future.

Therefore, for social networks to continue being a democratic space for opinion and information, it is necessary to identify the organicity of the debates. For the networks to become more transparent it is also critical to start identifying those responsible for this type of coordinated action, seeking to understand the interests behind the contracting of these automation services and propagation of misinformation.

BIBLIOGRAPHY

Many Americans Believe Fake News Is Sowing Confusion. Available at: http://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/

Bessi, A.; Ferrara, E. **Social bots distort the 2016 US Presidential election online discussion.** Available at: http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653

Pew Research Center. **News use across social media platforms 2016.** Available at: http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/ Accessed on August 02, 2017.

Wang, A. **Detecting Spam Bots in Online Social Networking Sites: a machine learning approach.** In: Foresti, S.; Jajodia, S. Data and applications security and privacy XXIV. Springer, pp. 335-342, 2010.

Brito, F.; Salvador, I.; Rocha, E. **Detecting social-network bots based on multiscale behavior analysis.** In: Seventh International Conference on emerging security information, systems and technologies. 2013.

Lee, K.; Eoff, B.; Caverlee, J. **Seven Months with the devils: a long-term study of content polluters on twitter**. In: Fifth International Conference on Weblogs and Social Media of the Association for the Advancement of Artificial Intelligence, 2011.

Ferrara, E.; Varol, O.; Davis, C.; Menczer, F.; Flammini, A. The rise of social bots. In: Communications of the ACM, v.59, n.2, 2016.

Davis, C.; Varol, O.; Ferrara, E.; Flammini, A.; Menczer, F. **BotOrNot: a system to evaluate social bots. 2016.**

Tavares, G.; Faisal, A. **Scaling-laws of human broadcast communication enable distinction between human, corporate and robot twitter users.** PLoS ONE v.8, n.7, 2013.

Varol, O.; Ferrara, E.; Davis, C.; Menczer, F.; Flammini, A. **Online Human-bot interactions: detection, estimation, and characterization.** In: Eleventh International Conference on Weblogs and Social Media of the Association for the Advancement of Artificial Intelligence, 2017.

Arnaudo, D. **Computational propaganda in Brazil: social bots during elections.** University of Oxford Working Paper, n.8, 2017.

Chavoshi, N.; Hamooni, H.; and Mueen, A. Identifying correlated bots in twitter. In Social Informatics: 8th Intl. Conf., 14–21, 2016.

Chu, Z.; Gianvecchio, S.; Wang, H.; and Jajodia, S. **Detecting automation of twitter accounts: Are you a human, bot, or cyborg?** IEEE Tran Dependable & Secure Comput 9(6):811–824, 2012.

Clark, E.; Williams, J.; Jones, C.; Galbraith, R.; Danforth, C.; and Dodds, P. **Sifting robotic from organic text: a natural language approach for detecting automation on twitter.** Journal of Computational Science 16:1–7, 2016.

Ratkiewicz, J.; Conover, M.; Meiss, M.; Goncalves, B.; Flammini, A.; and Menczer, F. **Detecting and tracking political abuse in social media.** In 5th Int Conf on Weblogs & Soc Med, 297–304, 2011.

Wald, R.; Khoshgoftaar, T. M.; Napolitano, A.; and Sumner, C. **Predicting susceptibility to social bots on twitter.** In Proc. 14th Intl. IEEE Conf. on Information Reuse and Integration, 6–13, 2013.

Matsubara, Y., Sakurai, Y., Ueda, N., Yoshikawa, M.: **Fast and exact monitoring of co-evolving data streams.** In: 2014 IEEE International Conference on Data Mining, pp. 390–399. IEEE, 2014

Ghosh, S., Viswanath, B., Kooti, F., Sharma, N.K., Korlam, G., Benevenuto, F., Ganguly, N., Gummadi, K.P.: **Understanding and combating link farming in the twitter social network.** In: Proceedings of the 21st International Conference on World Wide Web - WWW 2012, p. 61. ACM Press, New York, 2012

Tavares, G.; Faisal, A. **Scaling-laws of human broadcast communication enable distinction between human, corporate and robot twitter users.** PLoS ONE v.8, n.7, 2013.

Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. **Design and analysis of a social botnet.** 2012.

Wired. **How Twitter bots played a role in electing Donald Trump.** Available at: http://www.wired.co.uk/article/twitter-bots-democracy-usa-election Accessed on August 11, 2017.

The New York Times. **On Twitter, a Battle Among political Bots.** Available at: https://www.nytimes.com/2016/12/14/arts/on-twitter-a-battle-among-political-bots.html Accessed on August 11, 2017.

Deutsche welle. **The rise of political bots on social media.** Available at: http://www.dw.com/en/the-rise-of-political-bots-on-social-media/a-19450562 Accessed on August 12, 2017.

NY Daily News. **The billionaire GOP patron behind Trump's social media bot army.** Available at: http://www.nydailynews.com/news/politics/billionaire-gop-patron-behind-trump-social-media-bot-army-article-1.3236933 Accessed on August 12, 2017.

MIT Technology Review. **How the Bot-y Politic Influenced This Election.** Available at: https://www.technologyreview.com/s/602817/how-the-bot-y-politic-influenced-this-election/. Accessed on August 12, 2017.

Le Monde Diplomatique. **Entre trolls, robôs e ativadores: as eleições na internet.** Available in: http://diplomatique.org.br/entre-trolls-robos-e-ativadores-as-eleicoes-na-internet/. Accessed on August 12, 2017.

Founded in 1944, Fundação Getulio Vargas was created with the aim of promoting the social and economic development of Brazil, through the education of qualified administrators in both the public and private spheres. Over time, FGV has expanded its activities to other areas of knowledge, such as social sciences, law, economics, history and, most recently, applied mathematics, which is a benchmark in quality and excellence in all of its eight schools.

Luiz Simões Lopes Building (Main Office)
Address: Praia de Botafogo, 190 – Rio de Janeiro/ RJ
CEP. 22250-900
Tel: +55 (21) 3799-5938

EXPEDIENT

TEAM

Director
Marco Aurélio Ruediger

Researchers
Amaro Grassi
Ana Freitas
Andressa Contarato
Carolina Taboada
Danilo Carvalho
Humberto Ferreira
Lucas Roberto da Silva
Pedro Lenhard
Rachel Bastos
Thomas Traumann

Graphic Project
Arielle Asensi
Luis Gomes
Rebeca Liberatori Braga

Translator
Lucas Maciel Peixoto