CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*****.**

CYBERLAW
by CIJIC

EDIÇÃO N.º VIII – SETEMBRO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW

by CIJIC

CYBERLAW

by CIJIC

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, dada a pertença do CIJIC ao grupo do Network of Centers (https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic), a obrigação identitária desta comunidade, persuade-nos a publicar artigos em inglês. Traremos, portanto, duas investigações em anglo-saxónico.

Na oportunidade presente da publicação desta VIII Edição e dos actos legislativos nacionais em curso, foi nossa opção trazer uma visão jurídica sobre o poder, eventualmente, manipulativo da democracia através das redes sociais.

O contexto é o da eleição presidencial de 2018, no Brasil, mas o modo como se desenvolve, desde uma engenharia social mais dissimulada a uma difusão de *fake news* ou *deep fakes*, permitem utilizar tais distorção de forma globalizada. Sendo certo que carece de maior investigação o real efeito da *realidade* das redes sociais *versus* o do "*quotidiano não digitalizado*" e o resultado concreto disto em sede de apuramento final dos resultados de eleições livres e universais, parece já possível concluir que, mesmo ante esta condicionante ainda não determinada, a realidade democrática pode, efectivamente, ser *hackeavel*.

Não obstante, por princípio, a clarificação dos conceitos de *fake news* e *deep fakes*, deveria afastar-se do radical "notícia" que lhe dá a alma. Porque uma notícia corresponde a um acto jornalístico, exercício com tutela constitucional, que conclui um dado conteúdo factual, relatando acontecimentos de interesse geral da comunidade com o maior grau de objectividade possível. Uma notícia identifica-se pela clareza, simplicidade, exatidão, e pelo bom uso da língua em que é escrita. Compreende contraditório, ou a possibilidade deste, suporta-se em fontes credíveis. Há todo um ónus ético e deontológico que sopesa uma notícia assinada por um jornalista. Toda esta súmula é uma notícia. Comentário, mesmo televisivo, liberdade de opinião, todos os outros "*fenómenos*", não se identificam com este radical conceptual. Logo, porque continuamos a insistir em querer colar uma qualquer liberdade opinativa ao conceito de "notícia"?

Não vos soa ridículo o exercício de contínuo *fact-check* a exercícios de liberdade de opinião? Desde quando é que mentira foi legalmente proibida? Mas, pelo contrário, uma notícia que veicule um facto falacioso, de cariz subjectivo, não é fortemente sancionável? Desde logo pelos poderes de regulação, pela sindicância da própria classe, pelo público?

Será assim tão difícil perceber as diferenças?

Noutro plano, em efeméride do décimo aniversário da Lei do Cibercrime portuguesa, a Lei n.º 109/2009, de 15 de Setembro, olhamos para a perspectiva da aptidão do enquadramento legal, num contexto nada fácil, de obtenção de resultados eficazes em tempos, da acção *contra-legem versus* investigação, demasiado assíncronos. Qual a razão que explica a falta de enquadramento legal nacional para o agente (digital) encoberto, quando dezenas de outras polícias de investigação, congéneres, já o fazem?

Se há disciplina onde a soberania das fronteiras físicas acabou é no digital. Outrossim, pela fragilidade dos "muros" digitais e das deficiências do enquadramento jurídico-penal nacional, abordaremos ainda o fenómeno do *Ransomware*. Dez anos volvidos da Lei do Cibercrime, e em apologia à vanguarda em que já estivemos nos idos do início da década de 90 do século passado, impõe-se no presente, em 2019, o revisitar a especialidade da lei do cibercrime. O contexto presente de *leaks* de índole variada e processos mais ou menos mediáticos, reclamam prudência. A digitalização do Estado, por outro lado, impõem mudanças assertivas. Ademais, quer a falta da criminalização do roubo de identidade digital[1], quer a complexidade jurídico-penal do

[1] Atente-se por exemplo no Considerando (14) da Directiva: "(…) *A adoção de medidas eficazes contra a usurpação de identidade e outras infrações relacionadas com a identidade constitui outro elemento importante de uma abordagem integrada contra a cibercriminalidade. A necessidade de intervenção da*

Ransomware, quer a própria transposição da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 (esgotado o prazo de transposição no ano de 2015), quer a protecção do Estado digital (e não só) reivindicam melhores ferramentas, desde logo legais, que bem que poderiam servir de impulso necessário ao dormente legislador nacional.

Por fim, tema que não sai das agendas, o Regulamento geral de protecção de dados. Desta vez, as fricções que a ferramenta *blockchain*, cada vez mais usada no contexto das relações entre particulares e organizações, compreende face ao RGPD mas, e também, a melhor consecução dos objectivos proclamados pelo RGPD que esta ferramenta pode ajudar a alcançar.

Por fim, mas antecipando o futuro, atendendo ao propósito identitário da revista, passaremos nas próximas edições a publicar artigos de investigação dos alunos do Mestrado em Segurança da Informação e Direito do Ciberespaço, trabalhos estes desenvolvidos nas cadeiras que frequentarem.

Resta-me, neste final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, enereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido:

- Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2019

Nuno Teixeira Castro

União contra este tipo de comportamento criminoso poderá também ser ponderada no contexto da avaliação da necessidade de um instrumento transversal e abrangente da União.”

CYBERLAW

by CIJIC

DOUTRINA

CYBERLAW
by CIJIC

THE PUBLIC SPHERE (FORGED) IN THE ERA OF FAKE NEWS AND BUBBLE FILTERS: THE BRAZILIAN EXPERIENCE OF 2018

EDUARDO MAGRANI [1]

&

RENAN MEDEIROS DE OLIVEIRA [2]

[1] Doctor and Master in Constitutional Law from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio) and Senior Fellow at Humboldt University in Berlin, Alexander von Humboldt Institute for Internet and Society. Coordinator of the Institute of Technology and Society of Rio de Janeiro (ITS Rio). Research Associate at Law Schools Global League and member of the Global Network of Internet & Society Research Centers (NoC). Professor of the disciplines of Law and Technology and Intellectual Property at renowned universities such as FGV, IBMEC and PUC-Rio. Lawyer active in the fields of Digital Rights, Corporate Law and Intellectual Property. Author of several books and articles in the area of Law and Technology and Intellectual Property. Contact: https:linktr.ee/Eduardo_magrani

[2] Master's degree in Public Law and Bachelor of Law from the University of the State of Rio de Janeiro (UERJ). Post-graduate in Public Law from the Pontifical Catholic University of Minas Gerais (PUC Minas). Researcher at the Diversity Program at Getulio Vargas Foundation (FGV) School of Law and at the Fundamental Rights Clinic of the Faculty of Law of UERJ - UERJ Rights Clinic. Renan was an intern at The Center for Technology and Society at FGV School of Law. Contact: renanmedeirosdeoliveira@gmail.com

ABSTRACT

In this article we intend to explore, through the bibliographical review and the study of poll of voter intentions in Brazil, a little of the new technological phenomena that, together, affect the way in which the citizen forms his opinion about the everyday facts significant for public life, in general, the electoral process and the candidates, in a discerning way. Firstly, we take into account a brief approach to the theoretical framework in which we are based to think of a communicative, rational public sphere and in which the ideal situation of speech is sought. Secondly, we deal with the fake news - which is about false news that desires to influence the way the population looks at a particular candidate - and deep fakes - which have a similar goal but act by altering the reality in a more profound way. Finally, we approach how the algorithms, especially the use of bots, are acting in order to create a forged public sphere which does not match the real desire and the real need of individuals. In addition, we deal with how the thinking of individuals is being distorted in the filter bubble scenario, which potentializes the effects of the phenomena studied in the preceding items. Throughout the development of this study and through the hypothetical-deductive method, we will seek to demonstrate that the new technologies have a great potential of impact on the electoral will, although this potential has not yet been explored in all its extension. It walks into a scenario where the electoral process is hackable.

Keywords: Conected democracy; Fake News; Bots; Filter bubble scenario; Deep fakes.

RESUMO

No presente artigo pretendemos explorar, através da revisão bibliográfica e do estudo de pesquisas de intenção de votos, um pouco dos novos fenômenos tecnológicos que, juntos, impactam a forma como o cidadão forma sua convicção acerca dos fatos cotidianos importantes para a vida pública, de modo geral, e do processo eleitoral e dos candidatos, de modo particular. Em primeiro lugar, fazemos uma breve abordagem do arcabouço teórico em que nos baseamos para pensar numa esfera pública comunicativa, racional e na qual se busca a situação ideal de fala. Em seguida, tratamos das *fake news* – que se tratam de notícias falsas que buscam influenciar a forma como a população olha para determinado candidato – e das *deep fakes* – as quais têm objetivo similar, mas agem por meio da alteração da realidade de forma mais profunda. Por fim, abordamos como os algoritmos, sobretudo o uso de bots, estão agindo de modo a criar uma esfera pública forjada, que não condiz com o real desejo e com a real necessidade dos indivíduos. Além disso, tratamos de como o pensamento dos indivíduos está sendo distorcido no cenário das *filter bubble*, que potencializam os efeitos dos fenômenos estudados nos itens precedentes. Buscaremos demonstrar, ao longo do desenvolvimento deste estudo e através do método hipotético-dedutivo, que as novas tecnologias possuem um grande potencial de impacto na vontade eleitoral, por mais que esse potencial ainda não tenha sido explorado em toda sua extensão. Caminha-se para um cenário em que o processo eleitoral é *hackeável*.

Palavras-chave: Democracia conectada; *Fake News*; *Bots*; Filtros-bolha; *Deep fakes*.

1. INTRODUCTION

Fake news has previously demonstrated itself to be a powerful influencer in the electoral process. At the moment of forming his opinion, the voter suffers the impact of news whose truthfulness is not investigated, creating a judgment in relation to the candidates and the democratic process based on false news. It is not possible to affirm the exact dimension exercised by the fake news in the electoral process, but it is a fact that they exercise some influence.

The probable harmfulness of fake news is exponentiated when we consider how the new technologies are being used together. Deep fakes, algorithms, the filter bubble, among others, define the way you view reality, affecting aspects of life that go beyond elections. Questioning the status quo and veracity of incidents is something positive and essential in a democracy. However, it is necessary to have minimal consensus on facts, especially those of public interest. The great volume of news that puts in doubt the way things have been given in reality decreases the ability of people to differentiate the real from the invented.[1] It is indispensable that basic ethical standards are respected in order to ensure a minimally healthy democratic environment.

The scenario aggravates when one takes into consideration that traditional media, especially television, is losing space and confidence. The citizen does not believe in all that is said on TV anymore, believing the contents to be biased and out of context.[2] Television, in addition, exercises a significant role, but it must be taken into account that this role is being downgraded and space is being given to the internet, focusing on social networks. However, although the Internet is a source of tireless content and allows the search for information on the part of the user, the phenomenon that was perceived as filter bubble creates obstacles to a healthy and democratically desirable online dialogical environment.

In this article, we attempt to explore, a little of the phenomena that, together, impact the way

[1] Natalia Viana and Carolina Zanatta, 'Deep Fakes are Threatening on the Horizon, But They Are Not Yet a Weapon for Elections, Says Expert' *The Public* (16 October 2018) <https://apublica.org/2018/10/deep-fakes-sao-ameaca-no-horizonte-mas-ainda-nao-sao-arma-para-eleicoes-diz-especialista> accessed 25 October 2018 (Viana and Zanatta).

[2] The data demonstrated a clear generational distinction in relation to sources of obtaining information: the higher the age, the greater the use of television as the main means of communication. Up to 24 years of age, more than half of young people use the Internet as their main means. See the data of the Brazilian Media Survey 2016 (*Pesquisa de Media*, 2016) <https://bit.ly/2YH6udr> accessed 29 October 2016.

in which the citizen forms his opinion regarding the everyday facts important to public life and the electoral process and candidates. Firstly, we briefly outline the approach to the theoretical framework in which we think about a communicative, rational public sphere and in which the ideal situation of speech is sought. Secondly, we deal with *fake news* and *deep fakes*. In a few words, fake news is that news that seeks to affect the way the population looks at a given candidate. Deep fakes have a similar objective, they purely act by altering reality in a deeper way. Finally, we approach how the algorithms, specifically the use of bots, are acting in order to create a forged public sphere which does not match the real desire and the real need of individuals. In addition, we deal with how the thinking of individuals is being distorted in the filter bubble scenario, which potentializes the effects of the phenomena studied in the preceding items.

For the purposes sought here, we will broadly rely on the literature review on *fake news*, deep fakes, bots and filter bubble and on the impact of these phenomena in the elections and in the formation of the opinion of individuals. We will also be resorting to the survey of the intent of votes. Thus, we will seek to demonstrate, throughout the development of this study and through the hypothetical-deductive method, that the new technologies have a great potential for impact on the electoral will, although this potential has not yet been explored fully. It envisages a scenario where the electoral process is hackable.

2. BRIEF THEORETICAL NOTE: THE VIRTUAL PUBLIC SPHERE

One of the aims of this study is to point out the need for minimum ethical standards in the use of new technologies and mechanisms to circumvent the abuses arising from the utilitarian perspective, preventing the use of a person as a means and not as an end in itself. With this, we want to avert forms of manipulation of real profiles or the use of bots in order to create priorities forged in the public agenda. We can think of the most appropriate ethical perspective to deal with technology in a context in which democratic procedures and actions are related to the complex world of data and constant man-machine interaction in which we live. It is therefore essential to be ethical and moral not only on purpose but also to the entire procedure and range of actions.

For this,[3] we understand that it is necessary to take into account the complete and complex theoretical perspective of Jürgen Habermas, which allows us to think about the advancement of this new world of data in a dialogical and participatory way to achieve more legitimate and consensual regulatory proposals.

The German thinker, born in 1929, experienced in post-war Germany, with the Nuremberg trials, the depth of the moral and political failure of Germany in the realm of National Socialism.[4] Habermas stood out in the academic world by analyzing the development of the bourgeois public sphere from its origins in the halls of the eighteenth century, until its transformation through the influence of media directed by capital. [5]

For Habermas, the legitimacy of norms and the political system in contemporary capitalist Western capitalist societies depends on the acceptance of norms by citizens.[6] This occurs through successive attempts at justification in which each citizen must freely bind his will to the content of the norm through a rational and dialogical process of argumentation, that is, of reflection and conviction.[7]

[3] The main concepts and formulations of Jürgen Habermas and their relation with the internet platforms can be checked in a study by Eduardo Magrani, *Connected Democracy: The Internet as a Tool for Political-Democratic Engagement* (Juruá 2014) (Magrani).

[4] James Bohman and William Rehg., 'Jürgen Habermas' *The Stanford Encyclopedia of Philosophy* (2007) <https://plato.stanford.edu/entries/habermas/> accessed 29 July 2019.

[5] With the publication in 1962 of his habilitation, Jürgen Habermas, *Strukturwandel der Öffentlichkeit (Structural Transformation of the Public Sphere)* (English edn, Polity 1989).

[6] Jürgen Habermas. *Law and Democracy: Between Facticity and Validity*, vol 2 (2nd edn, Tempo Brasileiro 2003) 16 (Habermas).

[7] Joshua Cohen, 'Deliberation and Democratic Legitimacy' in James Bohman and William Rehg (eds), *Deliberative Democracy: Essays on Reason and Politics* (MIT Press 1997) 29.

In this type of society, the public sphere is precisely understood as the set of spaces that allow the occurrence of dialogical processes of communication, of articulation of opinions and reflective reconstructions of values, moral and normative dispositions that guide social coexistence. It is in the public sphere that the different constitutive groups of a multiple and diverse society share arguments, formulate consensus and construct common problems and solutions.[8]

The public sphere of Habermas comprises a zone of interchange between, on the one hand, the system – depicted as the world of work, guided by the logic of money and power, as an instrumental world of strategic action, noncommunicative, oriented by the market and bureaucracy[9] - and, on the other hand, the public and private spaces of the world of life - characterized as the world of interaction between people, which are organized communicatively through the ordinary language, enabling communicative action without a strategic action, oriented only to intersubjective understanding that ideally leads to agreement or leads to consensus.[10]

Habermas excelled in the academic world by evaluating the development of the bourgeois public sphere from its origins in the halls of the eighteenth century to its transformation through the influence of media directed by capital. The colonization would be the result of the meddling of politics and economy in the world of life, responsible for the reduction of citizenship and the transformation of the citizens into clients of social welfare services, that being the hallmark of modernity. In this scenario, the power of economic capital and politics invades the world of life destructively. According to Habermas, systemic intervention has a destructive impact on cultural reproduction, social integration and socialization as components of the world of life.[11]

While the author has not specifically and deliberately addressed the topic of the internet, we advocate the prospect of understanding digital platforms as abstract public spheres with great communicative and democratic potential.[12] We find in the digital spaces a public sphere in which individuals communicate regularly, through discussion forums, social networks, or

[8] Magrani (n 5).

[9] Jürgen Habermas. *The Theory of Communicative Action*, vol 2 (Beacon Press 1987) 113-197; Craig Calhoun (ed), *Habermas and the Public Sphere* (MIT Press 1992) 1-51.

[10] Habermas, *Law and Democracy* (n 8) 107.

[11] Although Habermas predicts that there is no complete shielding of the life-world of systemic logic, he believes that this logic can be nullified by the very dynamics of the world of life, based on communicative action.

[12] For an in-depth treatment of this defense, cf. Magrani (n 5) 25ff; The Habermasian theory alone does not sufficiently help us to deepen the possible solutions to these problems, since it was thought mainly to measure and induce the behavior of the rational and dialogic human agent that interacts in the public sphere. However, it serves as an excellent paradigm for analyzing the real possibilities of building a dialogue and speech scenario in the *online* context.

platforms for exchanging messages that nearly approach the conception of the public sphere drawn by Habermas on a smaller scale.

However, with the advancement of the most recent digital technologies, we have also followed the transformation of these connected spaces, and it is possible to envisage a possible reduction in their communicative democratic potential.

Today we observe the predominance in the connected spheres of profitable business models based on algorithmic filtration with the objective of conducting microtargeting practices, profiling, among others, directing the sale of products and services in a way Optimized for e-consumers. These current practices are based on the use to a large extent of the personal data of users and generate the aggravation of the effect called "Filter bubble", having harmful effects on democracy and braking the enthusiasm about the democratic role of the Internet as a public sphere for contemporary societies. In the following items, we considered some of these mechanisms and their ethical implications for the democratic context as a whole and for the elections in a specific way.

3. FAKE NEWS AND DEEP FAKES: DO THEY REALITY EXIST?

The fake news calls, fake news created for the purpose of misinforming, are hitting users with greater precision than expected. The type of content sent can also take into account the personal profile of those who will read the news in order to cause more direct impact, which is delivered by the microtargeting technique.

The fact is increasingly apparent that data produced by users on the Internet is being collected in some way by third parties. Not only personal data, but also what they read, research, and specifically, their consumption habits. At the same time, the Internet enables the massive uptake of these data if it is processing on a large scale. This large volume of data – structured, semi-structured or unstructured[13] – forms the big data, technology that allows people to know more and more individuals, and can even identify them personally by observing their habits, preferences and desires.

The richness of this information is such that it becomes inevitable to question how users allow such collection by consenting, for example, with the terms of use of websites and applications. It happens, firstly, that the terms of use are usually extremely technical and unintelligible to the general population, which makes the given consent not be completely conscious. Secondly, the performance of the companies itself is not always made transparently, that is, often the real purpose destined to the data is hidden from the users.[14]

With this and the increasing amount of data produced daily, the management of this information by third parties is worrisome. This is because big data goes far beyond a tangle of data: it is essentially relational. As individuals do not have control of their own personal data, it can be said that it belongs to those who collect them, creating a harmful vertical relationship.

Such technology opens an opportunity that has not gone unnoticed in the market. With this volume of data, there is a possibility of automatic personalization of content on digital platforms, including directing this filtering through targeted advertising, made possible through the tracking of cookies and by processes of retargeting, or programmatic media (behavioural re-targeting).

Companies observe the inputs generated by these data to guide their market policy in order

[13] Julia Lane and others (eds), *Privacy, Big Data and the Public Good: Frameworks for Engagement* (CUP 2014).

[14] About the terms of use on the internet, cf. Eduardo Magrani and others, *Terms of Service and Human Rights*: *An Analysis of Online Platform Contracts* (Revan 2016).

to achieve the desires and habits of consumers, through techniques such as tracking, profiling and targeting. This is done according to the behavioural trends analyzed, which leads to a targeting, therefore, of the market choices through the creation of targets. Today, we observe the predominance of the connected spheres of profitable business models based on algorithmic filtration in order to direct the sale of products and services optimally to e-consumers.

The microtargeting technique is a digital strategy for establishing the target audience through the collection of data from this audience so that the company can thoroughly know the profile in question. The strategy is done on top of a database assembled with information such as age, gender, hobbies, behaviour, among others. In principle, *microtargeting* was used in advertising marketing for the enhancement of products and services. Now there is talk of political marketing as it assists candidates to define a niche of specific voters by mapping possible supporters.

One of the advantages of microtargeting is to allow anticipating results that can be achieved at the end of the advertising or political project, delivering savings of time and money on the part of the agents, since their focus will be qualitative over what the targets actually want or need, dispensing with random attempts. These current practices, therefore, are guided by the use to a large extent of user data through big data that, in addition to making dishonest use of personal information, it can also generate political consequences, such as the worsening of the effect called "Filter bubble", harmful to the democratic role of the Internet as a public sphere, and the potentialization of false news.[15]

On this political-democratic context, some examples can help you comprehend how microtargeting is used to leverage false news. The paradigmatic case is that of the 2016 elections in the United States, hard impacted by the fake news. It is stated that the rumours largely assumed a negative content regarding Democratic candidate Hillary Clinton, in contrast to encouragement for the conduct of Republican Donald Trump. Fact is that, in 2016, 33 of the 50 false news on Facebook dealt with the political context lived in the United States.[16]

[15] On the relationship between fake news and elections, it is recommended to read the open letter advocated by the Coalition of Rights in the Network group, which provides guidelines on the subject. Open letter from civil society representatives from Latin America and the Caribbean on concerns about the fake news and elections, Coalition of Rights on the Network, ‘Fake News and Elections’ (*Rights on the Net*, 2017) <https://direitosnarede.org.br/p/carta-aberta-americalatinaecaribe-igf2017/> accessed 29 October 2017.

[16] Craig Silverman, ‘Here Are 50 of the Biggest Fake News Hits on Facebook From 2016’ (*BuzzFeed News*, 30 December 2016) <https://www.buzzfeednews.com/article/craigsilverman/top-fake-news-of-2016#.nl712lkw2> accessed 29 October 2018; ‘There are 7 Types of Fake News. Do You Know Them All?’ (*Magic Web Design*, 19 March 2018) <https://www.magicwebdesign.com.br/blog/internet/existem-7-tipos-fake-news-voce-conhece-todos/> accessed 29 October 2018.

Some false news has had such repercussions that they have run the world, like, for instance, that Pope Francis – and, therefore, the Roman Catholic Church – supported Donald Trump's candidacy, which would give him even greater support from the layers conservatives of American society. The rumour was disclaimed only when the Vatican spokesman made a public announcement saying that the pope never manifested such support and, neither, intends to take political positions.

Countries like Russia have also influenced the American electoral process. Among the rumours scattered, an army of "Russian trolls" published news that Hillary Clinton would be involved with satanic ritual practices. One of the narrative lines affirmed, upon alleged e-mails leaked between Hillary and his campaign manager, John Podas, that they participated in rituals with a priestess who adored the demon. It was, however, a performance of the artist Marina Abramovic on Spirit cooking, which was challenged in one of the hacked emails of the campaign.[17] Later, U.S. intelligence discovered that e-mails were hacked into an operation orchestrated by the Kremlin.[18]

However, a recent case that became emblematic and, in fact, aroused attention on how microtargeting can be used to disseminate false news, is that of the company Cambridge Analytica, appointed as one of the main vectors of viralization of fake news, as well as Donald Trump's victory in the elections.

The case begins with the creation of an application that ran on Facebook, thisisyourdigitallife, created by Cambridge Analytica scholar, Dr Aleksandr Kogan, active at the University of Cambridge, with the objective of developing academic research. For this, the app collected private information from the profiles of 270,000 users, with their consent, which until then was allowed and was in accordance with the terms of use of Facebook. It happens that, in 2015, the social network in question was validated that Cambridge Analytica had shared the data collected with a third party, the company Eunoia Technologies, which aimed at commercial purposes, in disagreement with the terms of use of the platform.[19] In this way, Facebook demanded that the information provided to third parties be destroyed, only thereafter

[17] Benjamin Lee, 'Marina Abramović Mention in Podesta Emails Sparks Accusations of Satanism' *The Guardian* (4 November 2016) <https://www.theguardian.com/artanddesign/2016/nov/04/marina-abramovic-podesta-clinton-emails-satanism-accusations> accessed 29 October 2018.

[18] 'How Russia-Linked Hackers Stole the Democrats' Emails and Destabilized Hillary Clinton's Campaign' *ABC News* (5 November 2017) <https://www.abc.net.au/news/2017-11-04/how-russians-hacked-democrats-and-clinton-campaign-emails/9118834> accessed 29 October 2018.

[19] 'Privacidade No Facebook: o que aprender com a Cambridge Analytica' (*Irisbh*, 19 March 2018) <http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/> accessed 28 October 2018.

it was discovered that Cambridge Analytica and other companies did not eliminate the information, which is why they would be suspended from operating on the platform from that moment on. At this point, nonetheless, the data of about 50 million Facebook users had already been compromised.

The scandal only came to the public in March 2018, when Christopher Wylie, who worked to get data from users on Facebook and passed it on to the company Cambridge Analytica (who was contracted internationally by several politicians in electoral times), issued Statements to the press, revealing that the profiles were gathered for the purposes of political manipulation in the connected public sphere.[20]

This case raises attention to some important factors. The App—thisisyourdigitallife functioned as a personality test that also financially rewarded those who agreed to participate. This represents a strong appeal to the user of social networks, who tends to want to satiate the curiosity of the results of these tests, which have become so common, even more by the possibility of earning some profit from it. In a masked manner, therefore, the company managed to collect a large amount of data, in a way that was consented to the use of a distinct purpose.

The secret purpose, it was later found out, was to collect data to chart voter profiles in order to use them for electoral marketing. This is nothing more than a microtargeting strategy, making use of the technology of the *big data* to attain a more refined material, suitable for producing even more precise results.

The company spent about US $1 million in data collection to send messages directed to specific voters, manipulating their political opinion through an algorithm that could analyze individual profiles and determine personality traits linked to the online behavior of the voter, as well as his feelings and fears, directed the content of sociopolitical manipulation based on these components. Therefore, an esteemed range of data collected by Cambridge Analytica was sold to political parties to, from an analysis, produce fake news capable of reaching the voter in what is most importante to him/her. That is, corroborating or attacking their more rooted positions, with the objective of dissuading them, with the certainty of success.

With this, it is essential to be clear that, in the final analysis, the big data is the individual in

[20] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 29 April 2017.

all its complexity and, therefore, one must have a critical conscience and think possibilities to regain control over personal data.[21] It is necessary to address judicial and extrajudicial forms of data protection, of the accountability of companies that carry out such activity. And, above all, to build a conscious use of the platforms in the users, so that they do not so easily give away their information in false exchanges of benefit, that turn against them in a way so painful for the society and the democracy in general.

Similar to the Donald Trump campaign in 2016, the Jair Bolsonaro campaign in 2018 in Brazil used several fake news to promote the candidate. The strategy became public when the press disclosed the existence of contracts of the candidate with private companies totalling about 12 million reais through which companies bought packets of message shots against the opposite party (PT) in WhatsApp, which comprised of the disclosure of false news.[22] The candidate also counted on the participation of groups of volunteer people who organized the creation and circulation of fake news.[23] The false news with the greatest repercussion during the elections concerned the "Gay Kit " and the fraud in the polls, and other news that circulated less dealt with the accusation that Fernando Haddad (PT) would be paedophile and that Jair Bolsonaro (PSL) would want to change the patroness of Brazil.[24]

Another way to come to subjugate the electorate is deep fake. The technologies already allow the recording of audios with imitation almost similar to the voice of people and the editing of videos in which the face of an individual who has never been in the situation appears as a participant. If in the daily scenario of non-public people, this is already extremely harmful to honour and image, this risk grows exponentially when we talk about public people. Audios and edited videos can be used, for instance, to defame the image of a certain candidate to an electoral position.

[21] Eduardo Magrani and Renan Medeiros de Oliveira, 'We are Big Data: New technologies and Personal Data Management' (2018) 5 CyberLaw 10-33 <http://www.cijic.org/publicacao/> accessed 29 July, 2019.

[22] Pedro Ortellado, 'Bias on the Internet Does Not Seem to Be Caused by "Bubbles"' (*Folha de São Paulo*, 2018) <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml> accessed 29 October 2018; Patricia Campos Mello, 'Entrepreneurs Campaign Against the PT by WhatsApp' (*Folha de São Paulo*, 18 October 2018) <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> acessed 29 October 2018.

[23] Mariana Simões, 'Pro-Bolsonaro Groups on WhatsApp Orchestrate Fake news and Personal Attacks on the Internet, Research Says' *El País* (24 October 2018) <https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9zXzmjDbYv5OkjAm1hVipWBURMCPyiOORIaxSsy_qNxEjzrpHKxfQ> accessed 29 October 2018.

[24] '"Voter Fraud" and "Gay Kit" Have a Greater Impact than Other Fake Twitter, Facebook and Youtube News' (*FGV DAPP*, 1 Novemeber 2018) <https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/> accessed 29 October 2018.

A recent case illustrates this possibility. On October 23, 2018, a video was circulated on the internet in which, supposedly, the candidate for governor of the state of São Paulo, João Doria (PSDB), appeared in intimate scenes with women. Five days after the second round of elections, the circulation of a video in this sense is enormously damaging to the image of the applicant, especially when it is considered that Doria is a defender of the traditional family. The then-candidate filed for investigation in Electoral Court. Initially, the investigations in relation to the video denoted that it would be assembly or simulation: expert report stated that the face of the candidate would have been wrongly inserted into the video, putting him in a situation in which he did not participate.[25] Subsequently, a new report punctuated the truthfulness of the video.[26]

This is a definitive case of deep fakes. Moreover, reality itself is called into question, and what is true or false is no longer known. This creates a mental confusion in the electorate, which happens to believe in one side without any solid ground. All being questionable, the human desire for an answer grasps at any clue of truthfulness - whether this clue is supported by some proven fact or only in self-deception.[27]

After the video was released, the voting intentions surveys showed some variation in the percentage points of each candidate. According to Datafolha's survey, on October 25 2018, Doria had 52% of votes, while on the 27th of that month it had fallen to 49%.[28] Considering the intensity of the campaigns in the days immediately preceding the elections and the profusion of information that is disclosed, we can not affirm that the video was directly responsible for this fall. In addition, the first forensic report disclosed indicated that the video would be an assembly or simulation, which may have caused more doubts in the voter. Fact is that the disclosure of this deep fake, accompanied by expert reports that did not indicate a single solution, was not enough to prevent the victory of the candidate, who won with 51.77% of the valid votes. Note, however, that we can affirm that the video was an important factor to be faced in the final moments of the campaign. In the current context, citizens are aware that there is an indiscriminate disclosure of *fake news*, so that they can consider, without any

[25] Sérgio Quintella, ‘Expertise Reveals Report on Intimate Video Attributed to João Doria’ *Veja São Paulo* (24 October 2018) <https://vejasp.abril.com.br/blog/poder-sp/pericia-aponta-montagem-em-video-intimo-atribuido-a-joao-doria/> accessed 29 October 2018.

[26] Redação Pragmatismo, ‘Intimate video of João Doria is true, new report points out’ (*Pragmatismo Político*, 26 October 2018) <https://www.pragmatismopolitico.com.br/2018/10/video-intimo-joao-doria-verdadeiro-pericia.html> accessed 29 October 2018.

[27] Eduardo Gianetti, *Lies We Live By: The Art of Self-deception* (Companhia das Letras 2005)

[28] Gabriela Fujita, ‘SP: Datafolha shows France with 51% and Doria, 49%; Ibope brings 50% for each’ *UOL* (Sao Paulo, 27 October 2018) <https://noticias.uol.com.br/politica/eleicoes/2018/noticias/2018/10/27/datafolha-ibope-sp-doria-franca.htm> accessed 29 October 2018.

evidence in any of the senses, that the disclosure of the video was merely a ruse of the opposition to discredit the adversary. Thus, they ignore whether the video was indeed true or false and cling to the beliefs already formed - which are often based on *fake news*.

In this context,[29] there are bills that seek to criminalize the disclosure of false facts during the electoral year, such as House Bill No. 9973/2018, 10292/2018, 9931/2018 and 9532/2018. The Senate Bill No. 246/2018 is broader and seeks to insert in the Civil Framework of the Internet "measures to combat the disclosure of fake content or offensive Internet applications." In addition, there are groups intended to accomplish fact-checking. But in a scenario where everything is questionable, who will check the truthfulness of the check on reality? The profusion of true and false information could lead to an "infocalypse," as Aviv Ovadya[30] warns. That is why we affirm above that it is essential to guarantee a minimum level of consensus on reality and a respect for fundamental ethical principles.

The impacts of this manipulation of the public sphere go far beyond the elections. In the long term, it may be that the elaboration of public policy-making is based on a forged popular will, generating state expenditures that do not meet the real needs of citizens. Moreover, the constant legitimacy of the actions of politicians can be forged, even if unattractive public policies are put into practice. In the following item, we made some considerations about the filter bubble and its impact on the opinion formation of individuals and the configuration of the public sphere.

[29] An exhaustive enumeration and detailed presentation of all bills on the subject would require its own study and would go beyond the limits of this article.

[30] Aviv Ovadya, ‘What's Worse Than Fake News? The Distortion Of Reality Itself’ [2018] 35(2) New Perspectives Quarterly 43-45.

4. THE PUBLIC SPHERE FORGED BY ALGORITHMS AND THE PERSONAL CONVICTION IN THE FILTER BUBBLE AGE [31]

Filter Bubble[32] can be defined as a set of data produced by all the algorithmic mechanisms used to make an invisible edition aimed at the customization of online navigation. In other words, it is a kind of personification of the contents of the network, made by certain companies like Google, through its search engines, and social networks, like Facebook, among several other platforms and providers. It is then formed, from the navigation characteristics of each person, a particular online universe, conditioning their navigation. This is done by tracking various information, including the user's location and cookie registration.[33]

With these techniques that generate the bubble filters, the internet would be transforming into a space in which is shown what is thought to be of interest to us. Thus, we are almost always hidden from what we really want or eventually need to see. Thus, it can be said that the filter bubble is paternalistic and prejudicial to the debate and the formation of consensus in the connected public sphere, being possible even to question its constitutionality, since it can suggest restrictions to fundamental rights, like access to information, freedom of expression, as well as the autonomy of individuals.[34]

Filtering has emerged as a necessity and is often considered welcome, generating a great deal of comfort for the user, who quickly and efficiently finds, in most cases, the information or any other content that he wants to access. This is Netflix's business model, for instance, which allows the user to have at his disposal a collection of movies based solely on his profile through the suggestion of personalized titles and filters, in order to improve his experience.

Though, beyond convenience, the problem lies in the form and in the excess of filtering, both by the companies and by the individuals themselves, who, unconsciously, restrict themselves and move away from contradictory perspectives, impoverishing, the value of the debate in the virtual public sphere. Consequently, bubble filters limit users to what they wish

[31] Some of the considerations made in this chapter were explored in Eduardo Magrani, ‘The Internet of Things: Privacy and Ethics in the Age of Hyperconnectivity’ (Pontifical Catholic University of Rio de Janeiro 2018); *See also* Magrani, *Connected Democracy* (n 5).

[32] Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You* (Penguin Press 2011).

[33] As Tim Wu notes in Tim Wu. *The Master Switch*: *The Rise and Fall of Information Empire* (Vintage 2011), “Cookies are, in a nutshell, access data that consist of the "digital footprints" left when passing through and manifesting through online environments.”

[34]A peremptory statement in this direction would require further study, so that the specific approach of this point would go beyond the limits of this study.

(or would like) according to, most often, an algorithmic prediction.[35] This creates a problem in accessing the information that should be seen to enrich the democratic debate.

Furthermore, from another perspective, the internet user, when navigating the most well-known sites, is today the target of a torrent of targeted advertising that signifies the commercial interest behind this filtering and personalization mechanism.

The internet is plastic and alterable, and the reality that we involuntarily become hostage to the algorithms that insert us into these bubbles has been seen as one of the most drastic but subtle changes because they are often indistinguishable. The filter bubble's premise is that the user does not unintentionally decide what appears to him within the bubble, nor does he have access to what is left out.

The information curation executed by traditional media, including offline media, already materializes the concept of content filtering by choosing and separating a series of information. Habermas, as well as other Frankfurt School theorists, such as Adorno and Horkheimer,[36] was in advance attentive to the traditional media force and its effect on modern democracy.[37] Nevertheless, internet platforms are often deficient of sufficient transparency in their informational and algorithmic clipping, giving consumers a false idea that information has a neutral and free flow. In addition, algorithm filtering in online environments allows for a degree of customization and targeting on a much larger scale,[38] which tends to accelerate with the coming of the Internet of Things,[39] given that with more and more intelligent devices connected around us, we will have even more personal data being collected, stored and treated.

In the light of the above, the idea that Internet infrastructure as a public sphere has the potential to allow the discussions to be strong enough to reach different segments and different interest groups, replicating through the various networks of people who make up society, may be an increasingly distant reality. This is due to the fact that the expressions are often restricted to the same network of people with common interests and communication channels easily negotiated by the platform holders. The conclusion of this is the broadening of communication fragmentation and the polarization of public debate.[40]

[35] Evgeny Morozov, *To Save Everything, Click Here*: *The Folly of Technological Solutionism* (Public Affairs 2013)

[36] Rolf Wiggershaus and others, *The Frankfurt School: Its History, Theories, and Political Significance* (MIT Press 1995).

[37] Habermas, *Law and Democracy* (n 8) 99.

[38] Magrani, *Connected Democracy* (n 5).

[39] Cf. Eduardo Magrani, *The Internet of Things* (FGV Editora 2018).

[40] As Cass Sunstein notes in Cass Sunstein, *Republic.com 2.0* (Princeton University Press 2009) and Cass

In a Habermasian view of legitimizing the political-democratic system, this scenario is unacceptable, since the minimally free communication flow must be preserved in the public space, allowing all those who may be reached to have a voice and participate in an increasingly direct way in decisions, whether appropriate to their private or political context in the public sphere. A quintessential example of this is the case of Cambridge Analytica, depicted in the previous item.

With the gain of greater sophistication and free-will of the technologies, our interaction with these agents will become more and more complementary and complex, bringing to the surface, still, a greater capacity of manoeuvring our thought and behaviour.

We must add to this—as a negative thing—the reality, that we often do not know how the algorithms of the intelligent objects we use and the virtual spaces in which we interact—work.[41] Each time these new nonhuman agents produce effects on our actions or even make significant decisions in our place through the customization of the information that is offered to us.[42]

Broadly speaking, decision-making and communicative democratic interaction today are undergoing an intensified transformation, as they suffer the intermediation and agency of non-human agents, such as robots or algorithms equipped with some degree of artificial intelligence. These elements are influencing our interaction and our discourse with the capacity to produce significant political-democratic material effects, so they should be better comprehended for regulatory purposes.

In political discussions, robots have been used across the party spectrum not only to win followers but likewise to conduct attacks on opponents and forge discussions. They manipulate debates, produce and circulate false news, and influence public opinion by posting and

Sunstein, *Republic.com* (Princeton University Press 2001), bubble filters would be a serious risk to the potential of the connected public sphere due to the lack of contact with dissenting opinions and the polarization of discourses leading to radicalism. This would be a problem with trends not to its resolution, but to its aggravation, from the sophistication of content customization algorithms.

[41] Frank Pasquale in Frank Pasquale, *The Black Box Society*: *The Secret Algorithms that Control Money and Informatio*n (Harvard University Press 2015) criticizes this situation by treating today's algorithms as black boxes and shedding light on the effects of this on a society guided in several areas by algorithmic data and decisions.

[42] In 2017, in Wisconsin in the US, a judge awarded a six-year prison sentence, taking into account not only the defendant's criminal record, but also his COMPAS score (Correctional Offender Management Profiling for Alternative Sanctions), which is a tool algorithm that aims to predict the risk of recidivism of an individual. The score suggested that the defendant had a high risk of committing another crime; so his sentence was six years. The defendant appealed the ruling, arguing that the judge's use of the predictive algorithm in his sentencing decision violated due process and is based on the opacity of the algorithms. Cf. Adam Liptak, 'Sent to Prison by a Software Program's Secret Algorithms' *The New York Times* (1 May 2017) <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?mtrref=www.google.com.br&gwh=B3F9140AAAB1DACDFCE11CBD55F4DB8F&gwt=pay> accessed 29 October 2017. The case went to the United States Supreme Court, which denied the writ of certiorari, refusing to consider the case.

replicating messages on a prominent scale. Many *bots*[43] have reproduced hashtags on Twitter[44] and Facebook[45] that gain eminence by massaging automated posts in order to strangle sudden debates on a particular topic.

Firstly, automated accounts can even confer positively to some aspects of life on social networks. The chatbots,[46] for instance, streamline customer service and, in some cases, even help consumers process their requests and get more information. Nevertheless, an increasing number of robots act with spiteful purposes in the public sphere. The social bots (social robots) are accounts controlled by software, which artificially generate content and establish interactions with non-robots. They attempt to imitate human behaviour and to pass as such in order to interfere in legitimate and voluntary debates and produce forged discussions.[47]

The growth of robot-led action thereupon represents a real danger to public debate, representing hazards to democracy itself, interfering with the process of consensus building in the public sphere, and in choosing representatives and government agendas.[48] For no other

[43] The term Bot, short for Robot (or Internet bot or web robot), is a software application that aims to provide an automated service to perform generally predetermined tasks. They mimic human behavior and are being used in politics and elections to influence opinion in digital networks, such as social networking platforms, instant messaging, or news sites. A conceptualization of the term can be found in Clara Velasco and Roney Sundays, 'What is a Web Robot and How Can it Influence the Debate in Networks? Experts Explain' (*G1*, 2017) <https://g1.globo.com/economia/tecnologia/noticia/o-que-e-um-robo-na-web-e-como-ele-pode-influenciar-o-debate-nas-redes-especialistas-explicam.ghtml> accessed 29 October 2017.

[44] According to the PEGABOT project, from the Institute of Technology and Society of Rio de Janeiro (ITS Rio) and the Institute of Equity & Technology, "[u] m Twitter Bot is an account controlled by an algorithm or script, usually used to perform tasks for example, retweet content containing particular keywords, respond to new followers, and send direct messages to new followers. Twitter Bots complex blogs can participate in online chatting and, in some cases, behave very much like human behavior. Bot accounts make up 9 percent to 15% percent of all active Twitter accounts, but more in-depth studies indicate that this percentage may be even greater because of the difficulty of identifying complex bots. Twitter bots are generally not created with malicious intent; they are often used to improve online interaction or service delivery by companies, governments and other organizations, so it's important to separate good bots from bad bots. <https://pegabot.com.br> accessed 27 October 2018.

[45] Robots are easier to spread on Twitter than on Facebook for a variety of reasons. An explanation on the subject can be found in Marco Aurélio Ruediger, 'Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018' (*FGV DAPP*, 2018) <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/> accessed 29 July 2019 (Ruediger).

[46] Institute of Technology and Equity, 'Experts Explain How the Robot can Influence the Debate in Networks' (*Medium*, 15 December 2017) <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849> accessed 29 October 2017.

[47] Ruediger (n 47).

[48] Bots account for more than 50% of the internet traffic around the world. Some bots are intended, for example, to require accountability of politicians, to root out causes for gender equality, or to help organize the (many) daily tasks of their users. Already other bots are aimed at spreading lies to influence conversations in the public sphere, a phenomenon that since 2014 has been gaining global scale. These bots are out there and hardly anyone knows how they work, who develops them and who they are funded. To illustrate this point, recent research has shown that the repercussion of the cancellation of the Queermuseu event, thoroughly commented on in the national press, has been inflated by robots on the internet. Of the more than 700 thousand tweets analyzed, 8,69% were triggered by bots, hampering public discussion. "While the decision to cancel exposure has taken other factors into account, it is possible to say that bot action has impacted on the way the debate was conducted, and its practical

rationale, there are bills in Brazil at the federal level to discourage the use and contracting of *bots* for electoral objectives, such as Senate Bill No. 413/2017, which strives to criminalize "the supply, hiring or the use of an automated tool that simulates or can be confused with a natural person to generate messages or other interactions, through the Internet or other communication networks, in order to impact the political debate or to interfere in the electoral process."

Confirming the thesis of risk to democracy, the Directorate for Public Policy Analysis (DAPP) of the FGV disclosed illegitimate interference in the online debate through the use of the 2018[49] and 2014 elections[50] and in public debates in general.[51] Scheduled accounts for massive postings have become a tool for manipulating social media debates. Here, it is significant to highlight that traditional media, especially television, have been suffering a constant process of wear and tear and discredit on the part of citizens. In this context, individuals to an increasing degree are using the Internet to acquaint themselves and trust in data obtained through the computer is superior to other media, such as newspapers, radio and television.[52] However, the *online* scenario is diffused by bots and algorithms that forge debate and change the priority of themes. In the course of the electoral race of 2018, automated accounts were responsible for 12.9% of interactions on Twitter.[53] In 2014, the first presidential election in which the robots had more meaningful performance, the interference was similar. The *bots* accounted for more than 10% of interactions on Twitter. Formerly during the Impeachment process of previous President Dilma Rousseff, the robots were answerable for 20% of the debate between supporters of Dilma. In the second round of the 2014 elections, 20% of the interactions in favour of Aécio Neves were brought forth by robots.[54]

consequences. (...) The use of the bots causes a polarization environment, since the internet has an increase in the flow of messages with the same content. In this scenario, says the researcher, it is difficult to come up with a spontaneous debate, with discordant and moderate ideas. 'This kind of action makes it difficult for more moderate positions to emerge. The search for a consensus is hampered because the robots can hijack part of the debate. " Cf. 'Research Shows that the Repercussion of the Cancellation of the Queermuseu was Inflated by Robots on the Internet' (*G1*, 2017) <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml> accessed 2 March 2017.

[49] Ruediger (n 47).

[50] 'Robots, Social Networks and Politics in Brazil: Analysis of Interferences of Automated Profiles in the 2014 Elections' (*FGV DAPP*, 2018) <http://dapp.fgv.br/en/bots-social-networks-politics-brazil/> accessed 29 July 2019.

[51] Ruediger (n 47).

[52] Special Secretariat of Social Communication, Presidency of the Republic of Brazil, 'Brazilian Media Research 2016: Habits of Media Consumption by the Brazilian Population' (2016).

[53]'Robot-Influenced Debate Reaches 10.4% on Twitter' (*FGV DAPP*, 19 October 2018) <https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciaveis-no-twitter/> accessed 29 October 2018.

[54] Ruediger (n 47).

With this kind of maneuvering, robots produce the false sense of broad political support for a specific proposal, idea or public figure, alter the direction of public policies, interfere with the stock market, spread rumors, false news and conspiracy theories, produce inaccurate information and content, as well as entice users to hateful links that steal personal data, among other risks.[55] Note, nevertheless, that saying that these bots work in favor of a given agenda does not mean that they "entirely dominate the network, nor that the consequent perception of the larger part of the people will be the straight result of the influence of these devices”.[56] What we ask to highlight are the dangers previously attained through the use of robots and the probable risks that are more and more close and reckless.

By interfering in developing debates in social networks, robots are directly reaching political and democratic processes through the influence of public opinion. Their actions may, for instance, create an artificial opinion, or unreal dimension of a certain opinion or public figure, by sharing versions of a particular theme, which expand in the network as if there were, among the part of society represented there, a very powerful opinion on a specific subject.[57]

The study of the use of robots already establishes clearly the adverse potential of this practice for the political dispute and the public debate.[58] One of the most apparent conclusions in this sense is the concentration of these actions in poles located at the extreme of the political spectrum, artificially promoting a radicalization of the debate in the bubble filters and, thereupon, undermining potential bridges of dialogue between the different political fields constituted. Therefore, the role of robots not only circulates false news, which can have damaging effects on society but also actively looks up to prevent users from informing

[55] On the existence today of an "army" of false profiles, cf. Juliana Gragnani, ‘Exclusive: Investigation Reveals Army of Fake Profiles Used to Influence Elections in Brazil’ *BBC News* (London, 8 December 2017) <https://www.bbc.com/portuguese/brasil-42172146> accessed 14 March 2018.

[56] Ruediger (n 47) 8.

[57] Yasodara Cordova and Danilo Doneda, ‘A Place for the Robots (In the Elections)’ (*JOTA*, 20 November 2017) <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017> accessed 9 March 2018.

[58] According to the research in Ruediger (n 47) 8 “The detection through machine learning occurs with the coding of behavior patterns from the collection of metadata. In this way, the system is able to automatically identify humans and robots based on the behavioral pattern of the profile. User metadata is considered one of the most predictable aspects of human and robot differentiation and can contribute to a better understanding of how sophisticated robots work. Identifying these robots or hacked accounts, however, is difficult for these systems. In addition, the constant evolution of robots causes the system, built from a static database, to become less accurate over time. However, it allows you to process a large number of complex correlations and patterns, as well as analyze a large number of accounts. The most efficient identification mechanisms combine different aspects of these approaches, exploring multiple dimensions of profile behavior, such as activity and time pattern. 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 robots accounts spend their time searching profiles and sending friendship requests.”

themselves suitably.

Another familiar strategy of automated profiles is the sharing of spiteful links, which is targeted at the theft of personal data or information. This information - such as profile photos - can be used to produce new robotic profiles that have features that help them start connections on networks with real users. A common action, which generally generates distrust about the performance of robots, is the marking by an unrecognized user.

This kind of action indicates that social networks, used by so many people for information purposes, may certainly and paradoxically contribute to a less informed society by manipulating public debate. Taken together, these risks and others represented by the action of non-human artefacts (such as *bots*) are more than enough to shed light on a real threat to the quality of debate in the public sphere,[59] especially since nonhuman artefacts have been gaining momentum, autonomy and behavioural unpredictability.[60]

[59] According to Habermas, *Law and Democracy* (n 8) 28-30, we must maximize the ideal speech conditions, that is, create an environment of democratic deliberation in which everyone has a voice. Faced with a scenario of crisis of representativity, the internet should be used as a tool for citizens to exercise their citizenship in an active way. According to Habermas, for democratic deliberation to occur, there are at least four conditions. These conditions, which characterize an "ideal speech situation", are basically linked to the need to guarantee the best conditions for deliberation and concern with the way the debate process is organized. They are: (i) each person must be able to express their own ideas openly and criticize those of others; (ii) the association of concepts of power and power with social status must be eliminated; (iii) arguments based on the appeal to tradition or dogma need to be exposed; and, as a consequence, the truth is achieved through the search for consensus.

[60] In this sense, it is paradigmatic the example of the robot Tay, chatbot with capacity of deep learning created in 2016 by Microsoft. The experiment proved to be disastrous and the robot had to be deactivated within 24 hours of its start: Tay began to disseminate hate speech against historically marginalized minorities, stating for example that Hitler was right and that she hated Jews. About Robot Tay, cf. Isabela Moreira, ‘Microsoft has Created a Robot that Interacts on Social Networks - and it has Become a Nazi’ (*Galileo*, 24 March 2016) <https://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-interage-nas-redes-sociais-e-ela-virou-nazista.html> accessed 29 October 2018.

5. FINAL CONSIDERATIONS

The latest developments in the new technologies addressed in this study alert us to the fact that the democratic role of the connected public sphere begins to run into risks and obstacles that can totally degrade its potential and should not be scrutinized enthusiastically as the panacea for salvation and legitimacy of the modern political system.

The hypertrophic impact of the market and bureaucratic economic rationality of the political system in the spheres of the world of life is seen by Habermas as one of the main pathologies of modernity, leading to loss of freedom and meaning in society.

Thus, the initial frenzy with the ideal of democratic virtual spheres and decolonization of the world of life provided by the new digital environments has lost its breath. Now that algorithms and other non-human agents are participating and influencing discourses in the public sphere, it is the question: will they be obligated to act morally and rationally-dialogically so that they do not negatively affect the ideal speech situation?

Many times there is a critical awareness of how the algorithms that make up the technologies work and how they can offer us personalized information from our personal data or even play upon our political vision. It is important to keep in mind that this operation often addresses political disputes or private business models that ask to maximize profit and not necessarily realize fundamental rights such as access to information, expression, and culture.

The Habermasian theory based on the logical and dialogical communicative concepts of the public sphere and ideal speech situation assists us to comply with how far we are distancing ourselves from a positive scenario from the perspective of democratic legitimacy. By the examination, we can conclude that the present situation is a colonization of the world of life established by non-human agents (bots, algorithms with artificial intelligence, among others) - and likewise by human agents, insofar as individuals also share and produce *fake news* and deep fakes-producing harmful consequences aggravated by the filter-bubble effects and the radicalization of discourses. Legal regulation must be attentive to these effects, seeking to correct them.

In the electoral context of 2018, fake news, in particular, and new technologies, in general, proved to be a challenging problem. On the one hand, controlling the broadcast and circulation of false news after its publication would be awfully dubious, given the rapid speed with which information is circulated in the context of the information society. On the other hand, prior analysis of the truthfulness of the news stories could imply institutionalized forms of censorship.

It is mandatory, therefore, to formulize institutional forms of combat against fake news without one of the fears mentioned above materializing. Thus, indirect regulations are more likely to be effective in countering fake news, such as banning countless fake accounts and setting ethical standards for the use of algorithms and artificial intelligence.

Note, nevertheless, that legislating on these issues is extremely complicated, as we are dealing with essential principles of democracy, such as freedom of expression and right of access to information. But this still seems to be the most appropriate alternative in the short and medium-term. There are technologies that can be used in smartphones and computers to realize the truthfulness of some information.[61] However, it is a technology of high value, which demands infrastructure and the replacement of devices that already circulate today. That is, it is a long-term measure and with many difficulties to be faced, such as those related to the privacy of technology users.

As we can observe, every day the new technologies are applying a greater influence on the life of the citizens and in the way they look at the facts. This impact expands more and more into all areas of our lives and has recently hit the elections thoroughly. Although it is not yet possible to say that algorithmic manipulation, bot use, fake news and deep fake disclosure are largely responsible for the election results, we can say that we are moving towards a scenario where it would be possible to hack the electoral process.

[61] Viana and Zanatta (n 3).

6. REFERENCES

Adam Liptak, ‘Sent to Prison by a Software Program's Secret Algorithms’ The New York Times (1 May 2017) <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?mtrref=www.google.com.br&gwh=B3F9140AAAB1DACDFCE11CBD55F4DB8F&gwt=pay> accessed 29 October 2017.

Aviv Ovadya, ‘What's Worse Than Fake News? The Distortion Of Reality Itself’ [2018] 35(2) New Perspectives Quarterly 43-45.

Benjamin Lee, ‘Marina Abramović Mention in Podesta Emails Sparks Accusations of Satanism’ The Guardian (4 November 2016) <https://www.theguardian.com/artanddesign/2016/nov/04/marina-abramovic-podesta-clinton-emails-satanism-accusations> accessed 29 October 2018.

Brazilian Media Survey 2016 (Pesquisa de Media, 2016) <https://bit.ly/2YH6udr> accessed 29 October 2016.

Carole Cadwalladr and Emma Graham-Harrison, ‘Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach’ The Guardian (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 29 April 2017.

Cass Sunstein, Republic.com (Princeton University Press 2001).

Cass Sunstein, Republic.com 2.0 (Princeton University Press 2009)

Clara Velasco and Roney Sundays, ‘What is a Web Robot and How Can it Influence the Debate in Networks? Experts Explain’ (G1, 2017) <https://g1.globo.com/economia/tecnologia/noticia/o-que-e-um-robo-na-web-e-como-ele-pode-influenciar-o-debate-nas-redes-especialistas-explicam.ghtml> accessed 29 October 2017.

Coalition of Rights on the Network, ‘Fake News and Elections’ (Rights on the Net, 2017) <https://direitosnarede.org.br/p/carta-aberta-americalatinaecaribe-igf2017/> accessed 29 October 2017.

Craig Silverman, ‘Here Are 50 of the Biggest Fake News Hits on Facebook From 2016’

(BuzzFeed News, 30 December 2016) <https://www.buzzfeednews.com/article/craigsilverman/top-fake-news-of-2016#.nl712lkw2> accessed 29 October 2018

Eduardo Gianetti, Lies We Live By: The Art of Self-deception (Companhia das Letras 2005)

Eduardo Magrani and others, Terms of Service and Human Rights: An Analysis of Online Platform Contracts (Revan 2016).

Eduardo Magrani and Renan Medeiros de Oliveira, 'We are Big Data: New technologies and Personal Data Management' (2018) 5 CyberLaw 10-33 <http://www.cijic.org/publicacao/> accessed 29 July, 2019.

Eduardo Magrani, 'The Internet of Things: Privacy and Ethics in the Age of Hyperconnectivity' (Pontifical Catholic University of Rio de Janeiro 2018).

Eduardo Magrani, Connected Democracy: The Internet as a Tool for Political-Democratic Engagement (Juruá 2014).

Eduardo Magrani, The Internet of Things (FGV Editora 2018).

Eli Pariser, The Filter Bubble: What the Internet is Hiding from You (Penguin Press 2011).

Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism (Public Affairs 2013)

Frank Pasquale in Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (Harvard University Press 2015).

Gabriela Fujita, 'SP: Datafolha shows France with 51% and Doria, 49%; Ibope brings 50% for each' UOL (Sao Paulo, 27 October 2018) <https://noticias.uol.com.br/politica/eleicoes/2018/noticias/2018/10/27/datafolha-ibope-sp-doria-franca.htm> accessed 29 October 2018.

Institute of Technology and Equity, 'Experts Explain How the Robot can Influence the Debate in Networks' (Medium, 15 December 2017) <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849> accessed 29 October 2017.

Isabela Moreira, 'Microsoft has Created a Robot that Interacts on Social Networks - and it has Become a Nazi' (Galileo, 24 March 2016) <https://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-

interage-nas-redes-sociais-e-ela-virou-nazista.html> accessed 29 October 2018.

James Bohman and William Rehg., 'Jürgen Habermas' The Stanford Encyclopedia of Philosophy (2007) <https://plato.stanford.edu/entries/habermas/> accessed 29 July 2019.

Joshua Cohen, 'Deliberation and Democratic Legitimacy' in James Bohman and William Rehg (eds), Deliberative Democracy: Essays on Reason and Politics (MIT Press 1997) 29.

Julia Lane and others (eds), Privacy, Big Data and the Public Good: Frameworks for Engagement (CUP 2014).

Juliana Gragnani, 'Exclusive: Investigation Reveals Army of Fake Profiles Used to Influence Elections in Brazil' BBC News (London, 8 December 2017) <https://www.bbc.com/portuguese/brasil-42172146> accessed 14 March 2018.

Jürgen Habermas, Strukturwandel der Öffentlichkeit (Structural Transformation of the Public Sphere) (English edn, Polity 1989).

Jürgen Habermas. Law and Democracy: Between Facticity and Validity, vol 2 (2nd edn, Tempo Brasileiro 2003) 16.

Jürgen Habermas. The Theory of Communicative Action, vol 2 (Beacon Press 1987) 113-197; Craig Calhoun (ed), Habermas and the Public Sphere (MIT Press 1992) 1-51.

Marco Aurélio Ruediger, 'Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018' (FGV DAPP, 2018) <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/> accessed 29 July 2019 (Ruediger).

Mariana Simões, 'Pro-Bolsonaro Groups on WhatsApp Orchestrate Fake news and Personal Attacks on the Internet, Research Says' El País (24 October 2018) <https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9zXzmjDbYv5OkjAm1hVipWBURMCPyiOORIaxSsy_qNxEjzrpHKxfQ> accessed 29 October 2018.

Natalia Viana and Carolina Zanatta, 'Deep Fakes are Threatening on the Horizon, But They Are Not Yet a Weapon for Elections, Says Expert' The Public (16 October 2018) <https://apublica.org/2018/10/deep-fakes-sao-ameaca-no-horizonte-mas-ainda-nao-sao-arma-para-eleicoes-diz-especialista> accessed 25 October 2018.

Patricia Campos Mello, 'Entrepreneurs Campaign Against the PT by WhatsApp' (Folha de São

Paulo, 18 October 2018) <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> acessed 29 October 2018.

Pedro Ortellado, ‘Bias on the Internet Does Not Seem to Be Caused by "Bubbles"’ (Folha de São Paulo, 2018) <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml> accessed 29 October 2018.

Redação Pragmatismo, ‘Intimate video of João Doria is true, new report points out’ (Pragmatismo Político, 26 October 2018) <https://www.pragmatismopolitico.com.br/2018/10/video-intimo-joao-doria-verdadeiro-pericia.html> accessed 29 October 2018.

Rolf Wiggershaus and others, The Frankfurt School: Its History, Theories, and Political Significance (MIT Press 1995).

Sérgio Quintella, ‘Expertise Reveals Report on Intimate Video Attributed to João Doria’ Veja São Paulo (24 October 2018) <https://vejasp.abril.com.br/blog/poder-sp/pericia-aponta-montagem-em-video-intimo-atribuido-a-joao-doria/> accessed 29 October 2018.

Special Secretariat of Social Communication, Presidency of the Republic of Brazil, ‘Brazilian Media Research 2016: Habits of Media Consumption by the Brazilian Population’ (2016).

Tim Wu. The Master Switch: The Rise and Fall of Information Empire (Vintage 2011).

Yasodara Cordova and Danilo Doneda, ‘A Place for the Robots (In the Elections)’ (JOTA, 20 November 2017) <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017> accessed 9 March 2018.

‘"Voter Fraud" and "Gay Kit" Have a Greater Impact than Other Fake Twitter, Facebook and Youtube News’ (FGV DAPP, 1 Novemeber 2018) <https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/> accessed 29 October 2018.

‘How Russia-Linked Hackers Stole the Democrats' Emails and Destabilized Hillary Clinton's Campaign’ ABC News (5 November 2017) <https://www.abc.net.au/news/2017-11-04/how-russians-hacked-democrats-and-clinton-campaign-emails/9118834> accessed 29 October 2018.

‘Privacidade No Facebook: o que aprender com a Cambridge Analytica’ (Irisbh, 19 March 2018) <http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/> accessed 28

October 2018.

‘Research Shows that the Repercussion of the Cancellation of the Queermuseu was Inflated by Robots on the Internet’ (G1, 2017) <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml> accessed 2 March 2017.

‘Robot-Influenced Debate Reaches 10.4% on Twitter’ (FGV DAPP, 19 October 2018) <https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciaveis-no-twitter/> accessed 29 October 2018.

‘Robots, Social Networks and Politics in Brazil: Analysis of Interferences of Automated Profiles in the 2014 Elections’ (FGV DAPP, 2018) <http://dapp.fgv.br/en/bots-social-networks-politics-brazil/> accessed 29 July 2019.

‘There are 7 Types of Fake News. Do You Know Them All?’ (Magic Web Design, 19 March 2018) <https://www.magicwebdesign.com.br/blog/internet/existem-7-tipos-fake-news-voce-conhece-todos/> accessed 29 October 2018.