



Human Security and Democracy: What's next for Brazil

Saulo José Casali Bahia

Member, Board of Trustees, WAAS;
Law Professor & Federal Judge, Brazil

Abstract

When discussing Human Security and Democracy, especially from a Brazilian perspective but also with global implications, it becomes essential to consider the impact and influence of what is commonly called cyber activism, which has started influencing public opinion and altered the approach to electoral outcomes. Thus, in contemporary societies, analyzing the exercise of democracy necessitates considering social control and efforts to combat intentional disinformation.

1. First Moment

Initially, cyber activism raised hopes for increased popular and citizen engagement by providing an alternative to conventional communication channels like radio, newspapers, and television. These social communication agents promoted direct interference in democratic and popular processes, due to the monopoly of the means of communication at their disposal, a monopoly that the State was always careful to preserve and regulate for the benefit and reproduction of the political game.

The *cybernetic activism* of the first phase broke with the access to information dominated by the traditional means of communication, and allowed the eruption of movements that were latent until then, since they were persecuted and left with an empty voice in the traditional press.

Initially, cybernetic activism appeared to be an ideal conduit for democracy, allowing every citizen an open role within social networks. What unfolded was a surge of movements in Brazil and globally, breaking free from previous constraints. The Arab world witnessed its *Spring*, with digital networks shaking traditional power structures, with the deposition of leaders and the renewal of parliaments. In Brazil, there was a powerful demonstration of *cyberpower* with the outbreak of the *Fora Dilma* (Brazilian former president) movement, which can be understood as the result of the very contradictions of the presidential regime, a minority in the world but adopted by Brazil and the USA—for example, and always a source of incessant crises.

Initially, there was an expectation of dialogue and interaction on social platforms—a promise of a brighter future through open, multi-subjective participation in networks. However, this vision diverged significantly from the reality presented by traditional journalistic networks, which often catered to those in positions of power.

There was an anticipation of heightened communication, quantitatively speaking, as cyberspace opened up to the information superhighway. Optimistic outcomes were envisioned.

John Perry Barlow even proposed a declaration of independence of cyberspace, stating: ‘Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.’

“Artificial intelligence as it exists today looks to the past, not the future.”

That was the thesis of the occasion, almost a return to direct democracy, which was previously only possible in small social groups. *Cyberspace* would become the new Greek Agora!

Some have also connected the Protestant Reformation from centuries ago, where each individual was able to carry out their own interpretation of the Bible, fleeing the interpretation dominated by clerical structures, with the cybernetic revolution taking place in the world today. The translation of the Bible into vernacular (national) languages facilitated access to evangelical knowledge for everyone, leading to fresh insights.

2. Second Moment

Soon after, however, other social and political phenomena began to draw attention. Like *Brexit* (the exit of the United Kingdom from the European Union), where it was perceived that there was a very high manipulation of social networks in the sense of wanting to stay or not in the unified European political and economic space. Similarly, this interference was observed during the 2016 North American elections and the 2018 Brazilian elections. In these instances, service providers, who possess data on social media users, manipulated speeches to impact network users. They achieved this by disseminating meticulously crafted, massive messages designed to evoke emotional responses and sway opinions. Advertising agents swiftly recognized the potential of this new digital landscape and stepped into the familiar role they had traditionally played in the media.

More access is not necessarily synonymous with better information. It was clearly verified by the formation of vertical communicative chains and the clear presence of interference and control in the informational flow. At times, it was even possible to perceive the automation of content production and reproduction, making public deliberation even more vicious.

Digital activism then showed its other face: of intense fragmentation of the public sphere and polarization, inevitable in the presence of antagonistic hegemonic groups.

3. Third Moment

The manipulation of information in social networks thus brought unprecedented regulatory challenges. Governments had to be called back to reestablish the democratic space already appropriated by *data brokers*, since there was no perspective on self-regulation by the subjects who interacted in the networks.

By the way, Luhmann speaks of the functional differentiation of politics, when, in the first phase, the public sphere was seen as a moral court of politics (17th and 18th centuries), fulfilling the role of integrating different points of view since it served for free and spontaneous public deliberation. In the second phase (19th and 20th centuries), the public sphere would serve as a democratic reinforcement to parliament, in the belief that public opinion would direct the actions of politicians. Finally, in the third phase (the 21st century), with *cyberspace*, there would be the fragmentation of the public sphere and the emptying of democratic deliberation, which is what we are currently experiencing.

“Fake news thrives because it caters to what we like and want to hear. All fake news has a truth: a connection with our values.”

The difference of opinions does not come close to the idea of integrating opposing points of view. There is polarization, radicalization and intolerance. This phenomenon, typical of *cyberspace*, has been the object of concern for governments and has been studied all over the world. In several countries, personal data protection laws have already been created with an attempt to establish authorities that can create regulation and control for the trafficking and appropriation of data. When you have free access to *cyberspace*, with the absence of brakes and restrictions, the possibility of collecting and using personal information by *data brokers* and *data units* arises. The use of psychometric algorithms, with the reconstruction of the users' profiles, allows for a comparative advantage and previously unimaginable advertising and suggestion initiatives. Knowing the most intimate desires of individuals in society, it is possible to direct information and create awareness among specific groups, creating *clusters* of people with the same values and preferences. These are the *social bubbles*, which will create a situation of self-reference where there is no circulation of new information but only the reinforcement of already known emotions. There is a kind of throwback to forums of like-minded people.

In this phase, with the free possibility of inserting information in the formed groups, the authority of the source (which existed in relation to the traditional means of communication) disappears, and there are no more interpretative parameters. There is erosion of the semiotic guarantors of the written texts because only similar visions circulate, reinforcing the known feeling.

When the individual manifests himself in *cyberspace* in favor of something (offering a *like*), when he shares the content of something, and even when he accesses or searches for something, he defines his profile and what he will start to receive (the same type of network information). The *cyberspace players* learn from the choices made, and will reinforce the *cluster/bubble* created, providing feedback to the user.

It is exactly similar to what happens with artificial intelligence, which by extracting prevailing data from the existing dataset, reinforces the patterns and biases already created. Artificial intelligence as it exists today looks to the past, not the future.

Communication becomes unilateral, even with the variety of sources that make it seem that there is a multilateral communicative character.

Our political thought becomes associative and affective, as it is associated with our desires, circulating no longer information, but emotion, which intensifies feelings and makes rational scrutiny disappear.

Precisely for this reason, *fake news* thrives because it caters to what we like and want to hear. All *fake news* has a truth: a connection with our values.

The *European Commission*, regarding *fake news*, has been trying to establish an important terminological differentiation, as there is *disinformation* (false news deliberately created to harm a person, social group, organization or country) and *misinformation* (when the false news is shared by people without knowing that it is false) or *malinformation* (news has a real basis but is modeled, aimed at causing harm, often attacking the private sphere).

4. Conclusion

The solution that governments envision involves creating a new legal framework for *data brokers*, a regulation for *cyberspace*, avoiding the verticalization and polarization that tend to happen, and abandoning reason for emotion.

A great example was the *Cambridge Analytica* episode, which involves *microtargeting* or consistent action in “*using data to change behaviour*”. With a small universe of individual data collection (300 thousand) around 90 million people were reached by the mere circumstance of the existence of links in social networks.

Democracy demands, therefore, the affirmation of the *right to informative self-determination*, where the protection of personal data is essential.

In Brazil, the national data protection authority was frustrated, despite the approval of the general data protection law. The compliance of companies is impeded in the name of cryptography, secrecy being justified on a false premise since virtual platforms are not mere intermediaries of information. They determine the content of the information, as businessman Mark Zuckerberg (Facebook) recognized in April 2018 in a 5-hour statement to the US Senate.

It is necessary to understand the real problem with social networks, and the existing risks to Democracy and Human Security, and the challenge posed to the use and manipulation of personal data in *cyberspace*.

Author's Contact Information
Email: saulo.bahia@trfl.jus.br