Panel: Norms, standards and good practices aimed at securing elections

The trolls of democracy

RAFAEL RUBIO NÚÑEZ

Professor of Constitutional Law
Complutense University, Madrid
Center for Political and Constitutional Studies. Spain

Democracy and its trolls

In the year 2000, Ulrich Beck published the book “Democracy and its enemies”. In this book, the German author warned us of how the geopolitical changes caused by the fall of the Berlin wall, posed a challenge to traditional models of democracy. From then onward we have witnessed the consolidation of even bigger changes, related to the impact of technology on wider society, and in particular, on the democratic process.

Blind faith in technology as an aid to democracy is being questioned, as we are increasingly faced with the dangers that technology poses for democracy. Algocracy, Dictadata, Weapons of Math Destruction, are just some of the many terms used to describe this threat, however, I am in no doubt that if this book was published again nowadays, it would be called “Democracy and its trolls”. Of course, here in Norway you are all too familiar with trolls, as ugly cave-dwelling creatures. Yet, the trolls I am talking about are less folkloric and choose rather to dwell on the Internet.

Although these dangers threaten the democratic process, they are analysed with particular pre-emption when it comes to elections. Technology is radically changing the way campaigns are carried out. This has always been the case, innovation has always been central to electoral campaigns. He who knows, understands and can uses new technologies has a competitive advantage, until everyone else adopts the same practices and they become normalised among all the candidates. Problems arise when technology stops being a competitive advantage and turns into a threat to the integrity of elections, inhibiting the right to free choice or altering the results from the ballot boxes.

In recent times, the electoral system and its fragility have been widely criticized worldwide. This fragility is directly linked to technology and affects the different phases of the electoral process: the nomination of candidates, in which the collection of signatures for independent candidates or the realisation of primary elections can be done via applications that risk creating problems that affect the process; the electoral campaign, impinging upon the free development of the voter’s will, the voting process itself, recounts and modifying or simply hampering results…

Following the most recent elections the debate has gained a whole new level of relevance, as its vital importance for democracy and the need to offer legal responses have been brought to light. Key examples of how current electoral regulation is not yet prepared for this new scenario include the Brexit referendum, and the North American electoral campaign. Each of these examples demonstrate that electoral regulation is not prepared for this new scenario.

Until now, there are very few countries that have taken this problem seriously enough and have changed legislation to provide a response to this phenomenon, and the rest have just tried to apply current legislation to the changing reality, which has ultimately led to legal insecurity. The problem is that these questions require a particular level of technical knowledge and understanding about the nature of the proceedings and their possible impact on the final result of the elections. Moreover, often there is a lack of empirical evidence on the real impact of these processes.

In addition to these factors, there is the hybrid character of threats that:

1. are developed on varying national and international planes
2. utilise a new concept of time, in which informative immediacy affects decision making.
3. Involve a variety of different actors: parties, media, citizens and private businesses, which stray from regulatory models exclusively centred on the role of the media and of parties.
4. Are carried out through actions that combine technological infrastructure and misinformation.

The final objective: the alteration of the final results of elections. Yet, the ways by which they erode confidence in the democratic system (for example by delaying recounts) and place doubt upon the legitimacy of elected officials are almost as important. Some have even asserted that these attacks seek reactions that would create greater limitation on the use of information, legitimising illiberal models of democracy.

Whatever the principal objective is, operators can be spoken about as the battlefield, websites and platforms as arms, and information as munition, thus it is not surprising that individuals such as Zuckerberg talk about it as an arms race to win the war of confidence.

But unlike the trolls you are familiar with here in Norway, these technological trolls do not just harm people but also processes and infrastructures. People see how their free will is impinged upon in the decision-making process, on the one hand through attacks on individual privacy, which allows for the adaptation of messages both in their advertising and in their other campaign techniques such as mailing, door-to-door canvassing and phone banking.

Traditional publicity has been replaced by new forms of communication that try to adapt messages to specific sections of the electorate as well as new communication channels. As a result, general messages have become increasingly personalized. Those that design campaigns no longer have to think about the masses, as the majority of individuals are already either convinced or lost. As such they must concentrate on the small group of swing voters, for which the campaign techniques gain a one-to-one (as in the 19th century) or many-to-many focus. They concern the specificity of data protection regulation; and the use of censuses and data bases; the purchase of online publicity, especially on social media during election periods.

On the other hand, the decision-making process is complicated by the creation and mass dissemination of false information through fake profiles, many of which are automated. Un recent study highlighted 48 million fake accounts on Twitter, of which 20.5 million are only active in the Mexican electoral process, and whose online activity is starting to bear resemblance to an episode of the Walking Dead.

The weight that interpersonal communication gains through social networks has led to the mass creation of bots, anonymous, automated and sometimes fake accounts that act as individuals online and increase the massive distribution of specific information, aiming to create currents of public opinion, acceptance or rejection of people or ideas, in an artificial way. By giving off the impression that they have widespread support, these features create a bandwagon effect, and others accept the ideas shared by this apparent majority. This generates herd behavior, by which individuals neglect personal responsibility and submit themselves to the will of the collective; they imitate one another and deny discrepancy. The redundancy of misinformation, especially when it is found in the mass media, is set up as a "belief", an unquestionable basis whose denial implies the risk of being disqualified.

As shown above, manageable and accessible tools are now widely used, allowing for the mass dissemination of information, which in turn impacts on the decentralization of information. However, "propaganda is still in the hands of those who can really produce it, whether that be States, governments, groups in power. (…) Propaganda is only effective if it is made in a professional way and those who have the ability to make propaganda are not individuals, but organizations, whether they be state organizations of otherwise." Although technology has empowered the individual and accelerated the exchange of ideas, it has also redistributed power such that it is concentrated in the hands of the few.

Individuals can also fall victim to data theft, as a result of cyberattacks to servers that seek to obtain private information, and strategically publish for media exploitation.

A clear example of the effect on proceedings is the alteration of census data that is available on electoral platforms, which can lead to duplicate votes, or prevent individuals with certain socioeconomic or ethnic characteristics from voting, generating chaos amongst certain voter communities.

Infrastructure can also be subject to attack, through the hacking of voting machines, the alteration of registration mechanisms in places where the vote is obligatory, or the alteration of mechanisms that process recounts (especially when there is no paper evidence of the vote). All these incidences place into doubt the role of the State as a guarantor of electoral security, especially in distributed systems.

When thinking about solutions, it is important to do so in a comprehensive way, in order to respond to the hybrid character of the threats, through bodies or individuals that are responsible for the comprehensive management of threats. It is not so much about providing a legal response but about a response in terms of public politics, including legal, defense, educational and commercial elements. And these measures should address the protection of proceedings, those who participate in them, and the infrastructures considered strategic and vital for national security, taking priority over the federal character of electoral proceedings in decentralized countries.

With regards to regulation, it should address five fundamental questions: 1. the actors involved in the campaign, the possibility of anonymity or the role that individuals can play, for example in the production of advertising favouring a certain political opinion; 2. The content of the campaign and the treatment of it (fake news, segmented publicity); 3. the channels used and the rules that can be established for these private spaces; 4. the timeframe of the electoral campaign and its limitation such as canvassing, the publication of information the day before the election, or during the ban on the publication of polls, and 5. The integrity of data (privacy).

There are currently two models of doing this. On the one hand, there is the model that argues for the free circulation of information as the maximum guarantee, focusing on assuring freedom of expression by guaranteeing transparency both of the people involved and of the way the campaigns are financed, as well as the tools that they use (such as algorithms). In many ways this harks back to the traditional approach of getting rid of trolls – shining light on them so that they turn to stone.

On the other hand, there are those who wish to avoid potential threats, with the risk that is posed by filtering truth from lies, and highlighting or even directly deleting fake content or unreliable sources. This responsibility may be delegated to the platforms themselves, under threat of a fine.

Both models require a swift reporting process and quick legal solutions that maintain the balance between the respect for guarantees and the attainment of the final objectives.

Another avenue to explore is that of autoregulation. The crisis of reputation and threat to the markets has forced platforms to adopt a set of measures in the past few weeks. Amongst them include:

1. Political and issue ads clearly labeled and allowed by authorized user only (based on identity and location)
2. An election commission to conduct an independent forward-looking assessment of the role played by Facebook in elections.
3. The deletion of fake accounts.
4. Approval of particular content and sources.

Although some warn that these measures, which have been adopted either voluntarily or to comply with the law, run the risk of placing the responsibility of guaranteeing fundamental rights in private hands, despite the fact that very similar practices can already be found in the field of intellectual property law.

Measures and codes of conduct

Cooperation is also essential. Operators and platforms should cooperate with electoral authorities, both in order to detect threats and to spread official information, as they have done in Panama and Mexico.

Intergovernmental cooperation: these incidents should be addressed as attacks against democracy and thus, an important element of the state agenda. Cyber attacks are a threat to democratic governments because “in an interconnected world, an online attack against a nation can be considered an attack against everyone” and governments should “create interstate behavioral norms and boost respect towards common global networks”. [1]

Cooperation between electoral authorities, academics and practitioners, in order to gauge the true impact of these actions and the efficiency of the adopted measures. This is something that Brazil has done, through the Advisory Council for Internet and Elections that advises the Electoral Tribunal.

Education allows us to confront this new reality, not just in terms of the functions of technology, but also in terms of its effects, teaching us to distinguish between the important and the irrelevant, between truth and lies, creating citizens that are capable of conversing and adopting rational points of view, something that is vital for democracy.

As I approach the end of my speech, I wish to highlight the complex problem that we are facing, and that the State alone cannot solve. A form of mass media, in a mature and full democracy, must guarantee freedom of expression, and be honest and truthful to the public that listens to it, sees it, or reads it.

A content platform or a social network, in a mature and full democracy, must guarantee the veracity of published content, or at least warn of the potential risks implied by certain publications or sources.

A citizen, in a mature and full democracy, must construct and reinforce criteria for the interpretation of information. In a hyperconnected society, the citizen gains a new responsibility, that of using the tools at their disposition to distinguish between fact and fiction and avoid spreading information when they are in doubt.

And the government in a mature and full democracy, like our own, must ensure that society can exercise their rights and liberties fully.

Thank you very much.

April, 2018