Strasbourg 21 November 2018

CDL-LA(2018)001*
Or. angl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

STUDY ON THE ROLE OF SOCIAL MEDIA AND THE INTERNET IN DEMOCRATIC DEVELOPMENT

by

José Luis VARGAS VALDEZ
(Substitute Member, Mexico)

**This document has been classified restricted on the date of issue. Unless the Venice Commission decides otherwise, it will be declassified a year after its issue according to the rules set up in Resolution CM/Res(2001)6 on access to Council of Europe d documents*

INTRODUCTION

David Kaye, UN Special Rapporteur for Freedom of Expression once stated: "*today, to be disconnected from the web is to be silenced*." The latest report by the Web Index shows that, for the second year in a row, the Internet and, more specifically, social media, has played a significant role in enabling social and political action, amplifying previously marginalized voices. According to Digital in 2017 Global Overview, half of the world's population now uses the internet, and the number of social media users grew by more than 20% over the past 12 months. There are now 2.7 billion of "active social media users."

People that engage in social media may use the Internet to organize and demand better services, more transparency and meaningful participation in the political arena (Santiso, 2018). Now, citizens can instantaneously talk to each other, speak up, organize and publicly share their concerns. Individuals all over the globe are now able to shape global perceptions, position topics in their national agendas and foster political activism. There are notable examples of this: from the Egyptian teenagers who used Facebook to rally protesters to Tahrir Square, eventually toppling the Mubarak regime, to the influence of fake news on the outcome of the Kenyan Presidential Election, to the Chileans who campaigned online to make overseas voting a key election issue with "Haz tu voto volar" or the fact-checking project "Verificado2018" in Mexico. This digital transformation is recasting the relation between States and citizens.

New technologies and social media have revolutionized the way people interact and exercise their freedom of expression and information, as well as other related - and sometimes conflicting - fundamental rights (Council of Europe, Resolution 1987 [2014]). In its beginnings, the Internet was hailed as an omen of equality and liberty, but the "democratization" of content production and the centralization of online distribution channels such as Twitter, Google and Facebook have had several unintended consequences: the proliferation of fake news, private and public disinformation tactics, and most importantly, the arrival of very powerful private actors in the democratic arena that literally own the information highways.

Even though these phenomena have existed since the dawn of the printing press, over the last few years they have become significantly more widespread and technically sophisticated, with bots, propaganda producers, fake news outlets exploiting social media and search algorithms that ensure high visibility and seamless integration with trusted content, misleading large audiences of news consumers, and more importantly, voters. In 2017 alone, 13% of countries holding federal elections have had their democratic process targeted by hacktivist, cybercriminals, and even public or private political actors, all of them with the intent to manipulate information, sway public opinion or even destabilize democratic institutions (CSE 2017).

Be it governments or non-State agents around the world, all have dramatically increased their efforts to manipulate information in social media with the intent of distorting online discussions and sometimes even suppressing political dissent. According to Freedom House's latest report, manipulation and disinformation tactics played an important role in elections in at least 17 other countries over the past year, damaging citizens' ability to choose their leaders based on factual news and authentic debate. This has an impact on the legitimacy of democracy itself and poses security challenges.

There are cases where State agencies have employed armies of "opinion shapers" to spread government views and counter critics on social media, or the case of Cambridge Analytica, which accessed and used private data of 50 million Facebook users, with specific intent and effects during electoral processes. Unlike other direct methods of censorship, such as website blocking or arrests for internet activity, online content manipulation is difficult to detect and even more difficult to defeat, given its dispersed nature and the sheer number of people and bots employed for this purpose.

In the past couple of years, foreign intervention in elections, through the use of social media, has also become a concern for democracies. Technological resources such as low-cost digital espionage campaigns, paid users and bots, selective disclosure of information or creation of

fake information has changed the rules of the game during electoral campaigns. As a side effect, this has eroded confidence in democratic governments.

At a global scale, these practices pose a major threat to democracies and question the idea of the internet as a liberating technology. They have constituted what Francis Fukuyama calls a "post-fact world… in which virtually all authoritative information sources were called into question and challenged by contrary facts of dubious quality and provenance." The result has been the widespread "belief in the corruptibility of all institutions" that "leads to a dead end of universal distrust" and hinders the possibility of democracy (Fukuyama 2017).

Given the potentially devastating effects of these practices on democracy and civil activism, it is necessary to outline solutions that ensure the legal, economic and political conditions for both internet freedom and fair elections to exist and develop. This research paper aims to analyze and describe, from a constitutional and regulatory perspective, how the Internet and social media have reshaped the democratic arena and the relationships among several principles and human rights involved in electoral processes, in order to identify possible solutions and good practices that foster the harmonious development of both the internet and democracy.

The main argument of this paper is that new information technologies have created a novel "public sphere" for the democratic debate, with new actors and conflicting rights that cannot be correctly addressed with the current understanding of human rights and democracy as an issue only between citizens and governmental institutions, or even as an exclusively national problem. Therefore, we require a different model based on principles of co-responsibility and international cooperation to regulate, adjudicate and solve fundamental rights collisions, to simultaneously protect social and individual freedoms in the era of e-democracy.

The first chapter will explore the extent to which the internet and social media have become a trusted and important source of political news and opinions, and a tool for political interaction and organization. In this sense, new technologies have reshaped the ways in which societies translate the will of the people into votes and representation. The worldwide pervasiveness of these new technologies has moved the arena of democratic debate to the virtual world, raising many questions about their influence on voter turnout and the need to surveil and regulate online social behavior. Even though the Internet fosters some aspects of the democratic game, it also hampers them.

In the second chapter, we will address the most relevant threats and legal dilemmas that entail the use of internet and social media in democratic processes. The analysis will be divided in two sections: first, it will focus on the challenges and risks that new technologies pose to *electoral democracy*, particularly cybercrime or cyberthreats clearly performed outside the legal boundaries; second, it will analyze the threats of such technologies to *deliberative democracy* when apparently used within the legal boundaries, and the legal dilemmas they have raised between freedom of commerce, personality rights (e.g. privacy and personal data protection), political rights (e.g. freedom of expression and vote) and democratic principles (i.e. fairness or equity in electoral campaigns). This chapter will also evaluate possible traditional solutions to these dilemmas and their shortcomings, to propose a new model based on principles and multiple regulatory approaches. Co-responsibility, adaptability and international cooperation are necessary to effectively guarantee a reasonable balance among all conflicting rights and democratic principles.

This study does not intend to provide concrete and universal solutions for all problems that might entail the use of the Internet and social media in all electoral processes. The particularities of each nation and each democracy would make it an impossible task (see Appendix B for examples of different criteria to solve similar problems). Instead, its purpose is to identify the most relevant legal problems caused by the use of those technologies, describe their logic and possible solution parameters, point out the shortcomings identified so far, and suggest a general set of principles and guidelines that might help to adapt democracy and its laws to the new technological realities. In this sense, the conclusion of this work resembles a roadmap to existing and future regulation and cooperation principles, rather than a handbook to solve all problems.

In many countries around the world this is quite a new topic and current electoral regulation is developing. However, if democracy is to be protected (along with its key components of freedoms and fairness) this novel sphere of human communication must be understood and governed. Protecting the constitutional framework while empowering personal, political and commercial freedoms requires a delicate yet necessary intervention of constitutional courts and congresses. The right balance between rights and freedoms is key for the legitimacy of institutions and, therefore, for the survival of democracy in this “post-fact world”.

CHAPTER 1
DEMOCRACY AND THE PERVASIVENESS OF NEW TECHNOLOGIES

According to the *Global Digital Report 2018,* more than half of the world's web traffic now comes from mobile phones. From a total of 7.6 billion inhabitants of the world, roughly 4 billion are Internet users (which represents 53% of the total population), and 3.2 billion are social media active users (which represents 42% of the total population). Most of them are concentrated in America, Europe and the Middle East:

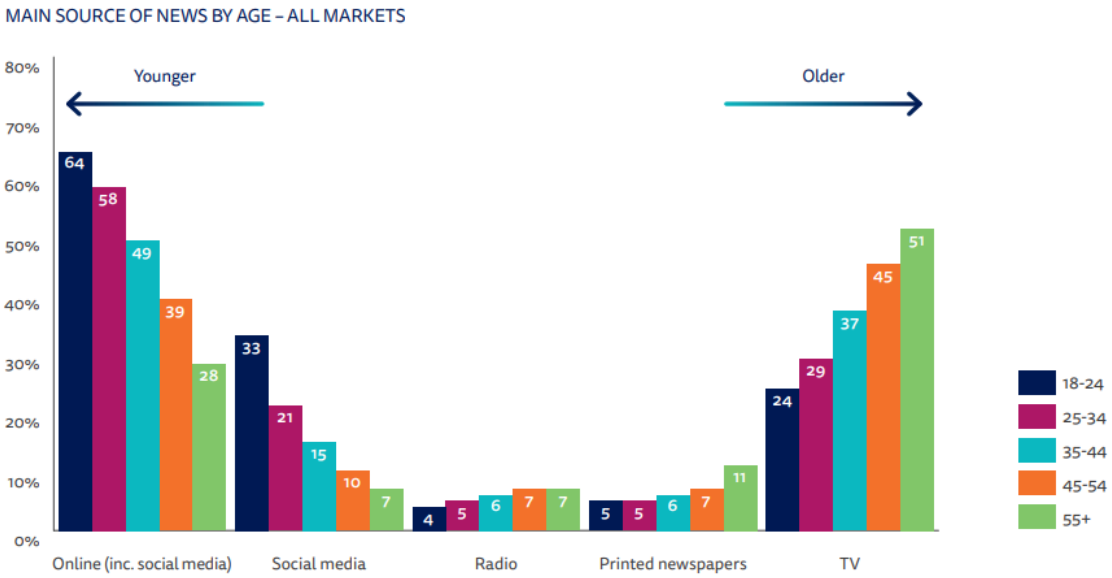
Region	Total population (millions)	# Internet users	% Internet users	# Social Network Users	% Social Network Users
Africa	**1,272**	435	34.2%	191	15.0%
America	**1,011**	741	73.3%	648	64.1%
Asia-Pacific	**4,214**	2,007	47.6%	1,779	42.2%
Europe	**843**	674	79.9%	448	53.1%
Midde East	**252**	164	65.1%	130	51.6%

Only between 2017 and 2018, the number of Internet users increased 7% and active social media users increased 13%. The average Internet user spends around 6 hours online each day. If we add this together for all 4 billion of the world´s Internet users, people will spend a massive 1 billion years online in 2018. Much of this time will be spent in social media platforms like Fabebook (with 2,167 million users), Youtube (1,500 millions), Instagram (800 millions) or Twitter (330 millions).

More surprising is that the Internet users' distribution among age groups is pretty even (see next chart). Along with the growing numbers of users, this might be helpful to explain the deep impact that the use of new technologies has had on basically every aspect of our lives. The use of the Internet has clearly permeated every layer of the social structure.

Internet users distribution by age group					
Age group →	**16-24**	**25-34**	**35-44**	**45-54**	**55-64**
% →	19.8%	19.2 %	20%	21.2%	19.8%

Even though everyone seems to use the Internet and social media, different age groups use them for different purposes. According to the *Reuters Institute Digital News Report 2017*, social media tends to be the main source of news for people between 18 and 34 years old, whereas television is more important for people above 55.

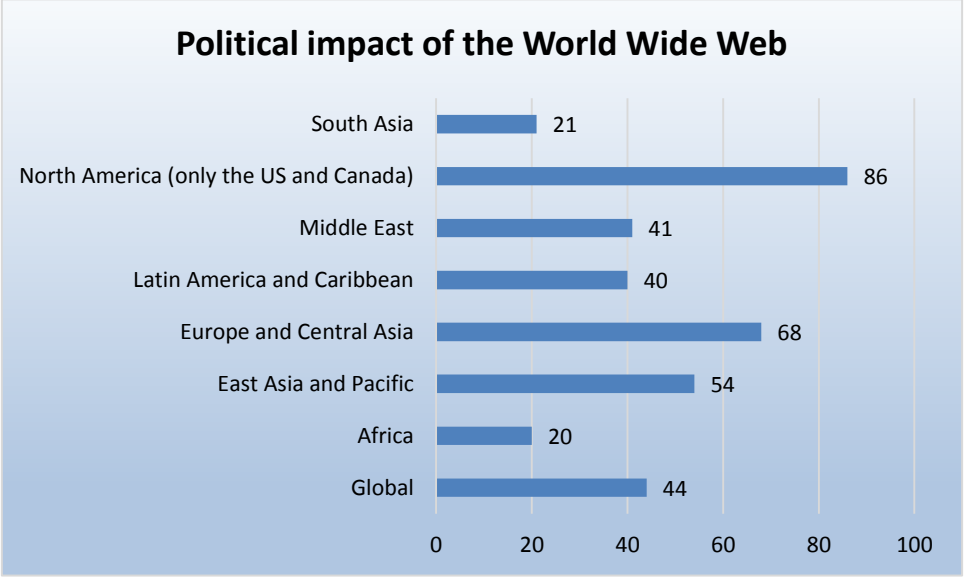


According to the same study of the Reuters Institute, more than half of the respondents (54%) prefer paths that use algorithms to select stories (search engines, social media, and many aggregators) rather than editors or journalists (44%). This means that young citizens might be making political decisions based on the information filtered by the algorithms of such digital environments, instead of on strict journalistic standards.

Nevertheless, "[t]he internet has quickly moved from primarily being used for information access to become a participatory environment more closely mimicking the democratic participation traditional in the physical world" (Laidlaw 2015, p. 7). As a consequence, the massive use of the Internet and social media platforms around the world is changing many aspects of our social and political life. Companies are migrating to more collaborative and horizontal business models that scatter both earnings and responsibilities (e.g. Uber, AirBnB). The social mechanisms of knowledge and opinion making are becoming more collaborative and self-regulated (e.g. Wikipedia, Facebook). And, as mentioned before, political activism has found new and efficient ways of organization and expression (Castells 2011; Cohen et al. 2012).

The Political Impact Index of the Webindex 2014 (World Wide Web Foundation 2014), provides interesting evidence of the deep impact that the use of the web has had in politics, public and private institutions. This indicator was applied throughout 86 countries and assesses the political impact of the internet by aggregating different measures of the following variables:

1. **Impact of open data on transparency & accountability:** Assesses the extent that open data has had a noticeable impact on increasing transparency and accountability in the country.
2. **Use of web-powered Information and Communications Technologies (ICTs) to catalyse action**: Assesses the extent that Web-powered ICTs have been used to catalyse social or political action.
3. **E-Participation Index**: Assesses the extent of the use of online services to facilitate provision of information by governments to citizens, and the interaction with stakeholders and engagement in decision-making processes.
4. **Impact of open data on government efficiency/effectiveness**: Assesses the extent that open data has had a noticeable impact on increasing government efficiency and effectiveness.
5. **Civil Society Organizations (CSO) use of ICTs to inform citizens**: Assesses the extent that major CSO use web-powered ICTs to educate and inform citizens about government decision-making and public policy issues.
6. **ICT use and government efficiency**: Assess the extent that the use of ICTs by the government has improved the efficiency of government services in this country.



This graphic shows the arithmetical means for every region, in which 0 means "none political impact" and 100 means "very high political impact".

When it comes to democracy, the Internet facilitates three aspects of it: electoral, monitoral and deliberative. "*Electoral democracy* is commonly known in the internet context as 'e-government'… *Monitoral democracy* refers to the bottom-up, grassroots activism that can be facilitated by the internet…. *Deliberative democracy* refers to participation by individuals in open debate in the belief that it will lead to better decisions on matters of common concern" (Laidlaw 2015, p. 10-11).[*] Regarding the first aspect, new information technologies make democratic processes more accessible to all citizens. From the electronic vote to the formation and actualization of centralized registries of voters, the Internet makes it easier for everyone to exert their political rights. As for the second aspect, these technologies allow large disorganized groups of people to organize and act to address specific social, economic or political issues. And third, as the Internet and new information technologies allow for greater transparency and accountability, as well as for broader and more efficient forms of political participation, they also extend the reach of the "public sphere" and strengthen deliberative democracy.

Social media in particular, understood as "internet platforms that allow for bidirectional interaction through users-generated content" (International IDEA 2014)[†], also have positive effects on democracy. They constitute the predominant platform of political debate and, as such, they are sources of political information (Democracy Reporting International 2017). According to a study by Bond *et al*. (2012) across 61 million Facebook users during the 2012 legislative elections in the U. S., the messages exchange among them had a direct influence on their political opinion, their web searches and even in their vote, and such influence extended to their "close friends". In a similar fashion, other studies suggest that the increasing flux of information fostered by social media strengthen the critical capacity of citizens towards their

[*] For the sake of a simple argument, we will consider the *monitoral democracy* variables as embedded in the *deliberative democracy* category. In the end, the citizens' capacity to surveil and self-organize for political purposes depends both on the information they can access and their possibilities to deliberate and agree on a common agenda.

[†] This study adopts a definition of social media as "web or mobile-based platforms that allow for two-way interactions through user-generated content (UGC) and communication. Social media are therefore not media that originate only from one source or are broadcast from a static website. Rather, they are media on specific platforms designed to allow users to create ('generate') content and to interact with the information and its source (International IDEA 2014: 11). While social media rely on the internet as a medium, it is important to note that not all internet sites or platforms meet the definition of social media. Some websites make no provision for interactivity with the audience, while others allow users only to post comments as a reaction to particular published content as discussions posts (or 'threads') which are moderated and controlled" (International IDEA 2014: 11).

governments (Gainous *et al.* 2016), and others suggest that there is a strong positive correlation (0.71) between the use of the Internet and social media, on one side, and the support to democracy as a desirable form of government, on the other (Basco 2018). And finally, many authors argue that the generalized use of internet and social media provides a more accurate knowledge of the citizens' interests and facilitates the organization of large scale social movements (Castells 2011; Metaxas and Mustafaraj 2012; Cohen *et al*. 2012; European Union 2015).

Access to the internet has become so important that "[m]any states, such as Estonia, Finland, France, Greece and Spain, have legislatively recognized internet access as a fundamental right". Moreover, "[a]ccess to the internet as a fundamental right received the United Nations (UN) stamp of approval in a report by Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (Laidlaw 2015, p. 20-21) and the European Court of Human Rights has ruled that Internet blocking may be "in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured 'regardless of frontiers'" (Ahmet Yıldırım v. Turkey, par. 67).

Nonetheless, even if "[t]he internet has the power to be a tool of democracy… its potential in this respect is at risk… [because the] same technology that facilitates discourse creates opportunities for censorship of information, monitoring of online practices and the subtle shaping and manipulation of behavior" (Laidlaw 2015, p. 1), hence threatening the authenticity of suffrage, the equity of the electoral competition and, ultimately, the capacity to translate the *will of the people* into institutional representation and governmental decisions. Given the enormous influence of the Internet in social interactions, this is not a minor concern.

The Resolution 62/7 adopted by the United Nations General Assembly on November 8th, 2007, states that democracy is a universal value based on the freely expressed will of people to determine their own political, economic, social and cultural systems and their full participation in all aspects of their lives. In the same sense, Article 21, third paragraph, of the Universal Declaration of Human Rights, declares that "the will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures".

In both instruments, the notion of "the will of the people" is the foundation of the legitimacy of the political, social and economic system adopted by a certain community. Par excellence, voting is the mean of expression of the popular will. The right to vote consists in the faculty of every citizen to manifest his or her will in favor of a candidate or proposal that represents, at least in a broad way, his or her own convictions. That is why one of the defining principles of a democratic vote is that it must be direct and free of interference (Fix Fierro 2005).

Even though the equivalence between the will expressed by the citizens in elections and the decisions taken by the public powers is not entirely absolute, representative democracy is a system of political organization that intends to translate the will of most of the people into concrete public policies or legislative acts. Hence, it is possible to ascertain that any element that threatens the *purity* of this will, is also threatening the internal validity and legitimation of an institutionalized social order. Any undue influence over the authenticity and freedom of suffrage might affect not only the translation of the popular will into concrete actions, but also the protection of minorities, the balance among basic human rights and the possibility to hold political parties and elected officials accountable.

Regardless of its positive effects on democracy, the internet and social media also have negative influences over the *purity* of the will of the people and, consequently, over the quality of democracies. First, the constant and simultaneous flux of information in real time across multiple platforms represent a huge challenge for the surveillance of behavior and resources during political campaigns. Second, the scattered and anonymous creation of content seriously difficult the identification and attribution of responsibilities for illegal online behaviors. Third, the growing use of *bots* and *trolls* to set agenda in the social media, as well as the massive

distribution of *fake news*, seriously damage the equity in the electoral competition and allow for external actor to manipulate the discourse and the voting preferences (Quintana 2016; Fidler 2017). And fourth, the algorithms that govern search engines and social media foster a partial and sometimes illusory comprehension of politics and democracy, because they provide biased information according to the interests and behavior of the users (Van Dijck 2013; McChesney 2013).

Given its unprecedented influence and efficiency in modulating social relations beyond borders and jurisdictions, the Internet and social media are very useful technologies to foster representative democracy. But unlike the traditional forms of power, these new technologies have democratized content production, have erased borders and jurisdictions and, most of all, have centralized the distribution channels in the hands of a few very powerful private actors. This is uncharted territory: owners of the information superhighways are powerful and deregulated enough to dictate conditions on social, individual and political freedoms, thus becoming a third actor in the democratic arena; and content production has become so "democratic" and anonymous that it is extremely difficult to identify trustworthy information and attribute responsibilities for illegal behaviors online. This context poses several challenges to guarantee the freedom of voting, fair elections, and most of all, the delicate balance among all rights and principles that preserve democracies. If citizens are unable to distinguish between false and true data and are unaware of the conditions under which they exert their rights and freedoms, the *purity* of their will might be compromised, as well as the democratic legitimacy of the social order.

One of the defining principles of a Liberal State is the minimum intervention of the State in the relationships among citizens, but the enormous influence of new technologies like the Internet and social media on democracy calls into question the reach of such principle (Coleman 2012; Gavara, de Miguel, Capodiferro 2015; Laidlaw 2015). We have seen several examples of the need to regulate social media behaviors around the world. For instance, on the *Tech for Good Summit 2018*, French President Emmanuel Macron reminded "the gathered Silicon Valley leaders of their responsibility to consumers and the world, in the wake of the recent scandals that have rocked companies like Google and Facebook" (Canales 2018). Likewise, on May 23th, 2018, the American federal Judge Naomi Reice Buchwald ruled that, since "the President [Trump] and Scavino exert governmental control over certain aspects of the @realDonaldTrump account, including the interactive space of the tweets sent from the account… [t]hat interactive space … is properly characterized as a designated public forum" and, consequently, any "viewpoint-based exclusion" of a person "from that designated public forum is proscribed by the First Amendment and cannot be justified by the President's personal First Amendment interests" (Breuninger and Mangan 2018).

However, the Internet regulation in the international realm calls for a complex and more nuanced discussion. The social order relies and flourishes also on economic freedoms and individual rights. To excessively limit those might also have an impact on other rights necessary for the survival of liberal democratic regimes, such as the freedom of information or speech. Furthermore, the fact a third set of actors (i.e. owners of information highways) has so much influence in electoral processes makes the ponderation of involved rights and freedoms even more difficult.

Given the conspicuous role of this third set of actors and the notorious difficulty of surveilling the vast global universe of the Internet, the question is no longer to what extent should the State intervene to protect political rights and the authenticity of the suffrage, but how should it settle the grounds to harmoniously protect economic and political rights, as well as social and individual freedoms, with the voluntary compliance of all involved actors and permanent cooperation of other nations.

To correctly address these new democratic and technological realities requires new regulatory models that allow for the right balance among all conflicting rights and principles, as well as for the normative recognition of the co-responsibility and interdependent rights of all those involved in making democracy possible. It calls for a model "open" enough to give voice to all interested parties, and "flexible" enough to enable the permanent adaptation of law to an everchanging

democratic, economic and technological reality.

CHAPTER 2
E-CHALLENGES TO DEMOCRACY

This section will address the most relevant challenges and legal dilemmas that entail the use of internet and social media in democratic processes. The analysis will be divided in two sections: first, we will focus on the challenges and risks that new technologies pose to *electoral democracy*, particularly cybercrime or cyberthreats clearly performed outside national legal boundaries; second, we will analyze the threats of such technologies to *deliberative democracy* when apparently used within the legal boundaries, and the correlative legal dilemmas they have raised between freedom of commerce, personality rights (e.g. privacy and personal data protection), political rights (e.g. freedom of speech and vote) and democratic principles (i.e. fairness or equity in electoral campaigns). This section will also evaluate possible traditional solutions to these dilemmas and their shortcomings, to propose a new model based on principles and multiple regulatory approaches.

Nations and private actors all over the world can easily use the Internet and new technologies to violate human rights or even as a military instrument to attack countries and their institutions through malware, ransomware, spyware and other sophisticated programs (Quintana 2016). This is known as "*cyber warfare*" and has been previously and successfully used to undermine State projects and systems, for instance the Stuxnet attack on the Natanz (Iran) nuclear plant (Quintana 2016; Mecinas Montiel 2016, p. 404, 418-419).

According to the Communications Security Establishment (CSE) of the Government of Canada, "[a]dversaries worldwide use cyber capabilities… Against elections… to suppress voter turnout, tamper with election results, and steal voter information… Against political parties and politicians... to conduct cyberespionage for the purposes of coercion and manipulation, and to publicly discredit individuals… [and] Against both traditional and social media… to spread disinformation and propaganda, and to shape the opinions of voters" (CSE 2017).[*] Furthermore, the CSE estimates that "it is highly probable that cyber threat activity against

[*] We have seen several examples of these interventions around the world:

- "In June 2016, the US state of Arizona shut down its voter registration system for nearly a week after adversaries attempted to gain access to the system. The next month, in Illinois, the state election agency took down its website for two weeks after discovering tens of thousands of voter records (e.g. names, addresses, and driver's licence numbers) were suspected to have been viewed by the adversaries" (Nakashima, as referred by the CSE).
- "Responding to perceived software vulnerabilities in its vote tabulation machines and warnings that the election may be targeted by Russia, the Netherlands amended voting procedures in their most recent election. To avoid the possibility of adversaries interfering with the election, all votes were hand-counted" (Escritt, as referred by the CSE).
- "In December 2016, adversaries gained access to the website of Ghana's Central Election Commission during the general election as the votes were being counted. An unknown adversary tweeted fake results that the incumbent candidate had lost. The electoral commission then sent out its own tweets claiming these results to be false. While the outcome of the election was not altered, this incident served to sow confusion in the minds of many voters" (BBC News, as referred by the CSE).
- "In the last US presidential election, both major political parties were subjected to cyberespionage attempts by Russia. Russian operatives used cyber capabilities to gain access to the emails of key political staff working on the Democratic Party campaign. The emails were subsequently leaked to embarrass the Democratic Party candidate" (ODNI, as referred by the CSE).
- "According to media reports, French intelligence believes that social botnets were used to influence the presidential election. Certain social media accounts, the same ones that were active during last year's US election, were promoting false and defamatory information against a leading candidate. In the final days of the election, one party was also victimized by the unauthorized release of thousands of campaign-related emails" (Auchard, as referred by the CSE).
- "Cyberwarfare, once a largely hypothetical threat, has become a well-documented reality, and attacks by foreign states are now a credible threat to a national online voting system. As recently as May 2014, attackers linked to Russia targeted election infrastructure in Ukraine and briefly delayed vote counting" (Springall *et al.* 2014).

democratic processes worldwide will increase in quantity and sophistication" over the next years for the following reasons (CSE 2017):

- *Many effective cyber capabilities are publicly available, cheap, and easy to use.*
- *The rapid growth of social media, along with the decline in longstanding authoritative sources of information, makes it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media and influence voters.*
- *Election agencies are, increasingly, using the Internet to improve services for voters. As these services move online, they become more vulnerable to cyber threats.*
- *Deterring cyber threat activity is challenging because it is often difficult to detect, attribute, and respond to in a timely manner. As a result, the cost/benefit equation tends to favour those who use cyber capabilities rather than those who defend against their use.*
- *Finally, there is a dynamic of success emboldening adversaries to repeat their activity, and to inspire copycat behaviour.*

Along with their accessibility, sophistication and public appeal, cybernetic tools are embedded in a borderless environment: The Internet. All the information flowing in the *web* could be potentially created, stored or constantly moved to any or many servers in the world, some of them located beyond any national border (e.g. international waters). What was legally created under national laws, could now be illegally allocated in a different jurisdiction or vice versa. Moreover, with the increasing use of *cloud computing*, the online information has become even more fragmented, thus making it extremely difficult to identify its origin or authorship. Cybercrime and cyberthreats operate beyond the limits of any national jurisdiction. This situation presents several difficulties to criminal investigation and prosecution; hence, the urge to attend this phenomenon from a transnational perspective (Davara 2003; Salt 2017 p. 520-521).

2.1 Cybercrime and electoral democracy

The concept "*electoral democracy"* refers to the institutional activities and infrastructure that make elections possible. From the organization of the election itself, to the creation and administration of voters' registries or the implementation of electronic ballots and internet voting, the electoral aspect of democracy sets the material and institutional conditions necessary to translate the popular suffrage into the appointment of representatives or the approval of laws and public policies.

It is quite evident that the feasibility and development of such activities are necessarily bound by technology. Moreover, new information technologies make democratic processes more accessible to all citizens. The Internet and social media might allow many people to exert their vote, express their opinion, organize for political purposes and even surveil the performance of public institutions and elected officials at a relatively low cost. But, as we have seen before, the use of new technologies could also entail new forms of illegal behavior, such as tampering with democratic processes, stealing voter information and cyberespionage.[*] These cybercrimes directly violate the right to privacy, threat institutional stability, hamper democratic governance, and constitute obstacles to the development of electoral democracy and to the use of technology to strengthen political rights.

The CSE has identified at least three areas in which electoral democracy, and particularly I-voting, could be vulnerable to cyberattacks (CSE 2017): First, if "voter registration occurs online, adversaries could use cyber capabilities to pollute the database with fake voter records… render the website inaccessible or have it display misleading information… erase or encrypt the data and thereby make it unavailable", or even steal information from the voter database "resulting in a massive breach of privacy". Second, the "internet voting presents many

[*] The legal status of spreading disinformation and propaganda to influence the opinion of voters is not so clear. Any regulation or ruling on these actions must consider a delicate balance between freedom of expression and commerce, on one side, and electoral equity on the other. We will discuss this issue in the next section.

more opportunities to adversaries… to 'stuff the ballot box' or to render the voting website inaccessible". And third, "adversaries could use cyber capabilities to disrupt or change the vote results while they are in transmission", thus directly damaging the electoral integrity and the legitimacy of the results.

For at least two decades, many countries have experimented with internet voting to strengthen political rights. For instance, in the year 2000, Switzerland launched the project "vote électronique" to test its reliability. Since then, the country has conducted more than 150 trials at the federal level and some cantons have made e-voting available for their citizens. In 2008, Norway also started testing internet voting and made some trials during the 2011 municipal elections and the 2013 parliamentary elections. In Canada, internet voting is available in some provinces (Ontario and Nova Scotia) since 2003. Perhaps the most successful experiment has been carried out by Estonia, where discussions about internet voting began in 2001 and since 2005 it has been considered as an additional and legally binding form of voting (ACE Project 2018).

Notwithstanding the success of some trials, the use of the internet for casting votes have raised several security concerns, even in the most experienced instances, such as the Estonian case. "Estonia was the first country in the world to use Internet voting nationally, and today more than 30% of its ballots are cast online", but researchers from the University of Michigan and the Open Rights Group have found "that the [Estonian] I-voting system has serious architectural limitations and procedural gaps that potentially jeopardize the integrity of elections" to the extent that "attackers could target the election servers or voters' clients to alter election results or undermine the legitimacy of the system." Their concerns were such that they concluded that "[s]omeday, if there are fundamental advances in computer security, the risk profile may be more favorable for Internet voting, but we do not believe that the I-voting system can be made safe today" (Springall *et al.* 2014).

The fact that almost two decades of building a safe system of Internet voting still raises such concerns suggests that there is still much work to do regarding cybersecurity and elections. The urge to address this challenge becomes even more pressing for several reasons. First, as abovementioned, because "it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication" over the next years. Second, because some countries may be fostering such aggressions, as could have been the case of the cyberattacks in the Netherlands, the US or Ukraine elections. And third, because these cyberthreats undermine fundamental human rights like privacy, and erode electoral integrity and democratic legitimacy.

There is no doubt that tampering with democratic processes, stealing voters' information and cyberespionage must be forbidden. However, the fact that these offences are performed in a borderless environment such as the Internet makes them a transnational problem and poses several legal challenges related to national sovereignty, the principle of territoriality, and access to remote data to constitute proofs and attribute responsibilities.

Most online information is rarely stored in the device where it was originally created; hence, making it extremely difficult to trace its origin or author without the cooperation of the *Internet Service Providers* (ISP) operating in other jurisdictions. Getting the ISP to comply with a foreign authority request could be particularly complicated (Salt 2017). First, because the requesting authority has no coercive power in a different jurisdiction. Second, because what is illegal in one jurisdiction might not be so in a diverse one. Third, because even if the ISP is willing to cooperate with the foreign authority, local regulations or contractual terms might require the authorization of the author of the information. This, of course, raises the question of whether the author could be forced to acquiesce to the request, given his/her right to refrain from giving any information that could incriminate him/her. And fourth, because directly requesting information to a private person in a foreign country without following the official institutional channels convened in international instruments, could be interpreted as a breach to national sovereignty; whereas complying with such procedures could jeopardize the efficiency of the investigation.

The obstacles to accessing and documenting information and data stored in foreign

jurisdictions have produced some relevant case-law rulings and even the adoption of peculiar legal strategies. In the case “Microsoft vs United States”, the software company refused to comply with a prosecutor’s request to access the data of a client’s e-mail, arguing that such information was stored in a foreign jurisdiction (Ireland) and granting access to it would represent a breach to sovereignty of another country. The judge in charge of the case ruled in favor of the US government, albeit there is still a pending appeal (Salt 2017, p. 542-543). In Mexico, a political party sued a website called “pejeleaks” for divulging defamatory content on the internet. However, the administrative electoral authority discarded the complaint arguing the lack of probatory elements to identify the authors of such content. In the consequent appeal, the High Chamber of the Federal Electoral Tribunal ruled in favor of the political party and order the administrative authority to conduct a deeper investigation even with the help of the Attorney General’s office (ruling SUP-REP-95/2018).

Accessing this kind of information can be so complicated, that some countries choose to adopt less formal strategies. For instance, in the case “Gorshkov-Ivanov”, two Russian hackers accessed and stole confidential information from several American companies and used the data to commit fraud and blackmail. In this case, the United States authorities took a different course of action: instead of requesting information from the Russian authorities, they cheated the hackers into traveling to the US to attend a fictitious employment offer and into providing access to their computers in the Asian-European country. The American authorities garnered enough information to convict the Russian hackers (Salt 2017, p. 540-542).

For at least 30 years, specialists have discussed possible solutions to these challenges, but haven’t agreed on a definitive answer. The Recommendation R(89)9 on Computer Related Crime and Final Report of the European Committee on Crime Problems in 1990 set the basis for discussing them. Five years later, the Committee of Ministers of the Council of Europe approved the Recommendation R(95)13 and highlighted the need to harmonize national procedural regulations in order to generate new tools to garner digital evidence across different jurisdictions. But it was the Convention on Cybercrime ETS No.185 (“Budapest Convention”) of the abovementioned Committee of Ministers, adopted in its 109th Session on 8 November 2001, that considered concrete and legally binding principles of transnational cooperation and solutions to these challenges. Countries like Portugal or Belgium have approved procedural legislation that replicate or even extend the provisions of the Budapest Convention (Salt 2017). So far, the articles 23, 31 and 32 of the Budapest Convention provide the following principles and solutions:

> *“**Article 23 – General principles relating to international co-operation***
> *The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.*
>
> ***Article 31 – Mutual assistance regarding accessing of stored computer data***
> 1. *A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.*
> 2. *The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.*
> 3. *The request shall be responded to on an expedited basis where:*
>   a. *there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or*
>   b. *the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.*

Article 32 –Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

In a few words, the Budapest Convention establishes two ways to access and document online information located in a foreign jurisdiction: by requesting the other party's co-operation "through the application of relevant international instruments" and "on the basis of uniform or reciprocal legislation, and domestic laws"; or by directly accessing publicly available information or restricted information with "the lawful and voluntary consent of the person who has the lawful authority to disclose the data", as long as such information is accessible through computers located on the requesting party's jurisdiction. Even though these provisions are helpful to solve the question of international cooperation and the limits of national sovereignty, they still have some relevant shortcomings: first, the possibility of international cooperation depends on legislative uniformity, hence posing the problem of what is illegal in one jurisdiction might not be so in a diverse one; and second, the Convention is not clear enough about who is the person with "*the lawful authority to disclose the data"*, thus granting enormous power to the ISP with the possible collateral damages to the legal rights of the author of such information. The solution to both shortcomings ultimately depends on the constitutional, legislative and judicial policies of each jurisdiction and, therefore, remains in the sovereign realm of each nation. Given the borderless and ubiquitous nature of the Internet, international collaboration and legislative uniformity are necessary conditions for the efficient investigation and prosecution of cyberthreats to democracies.

To face these challenges, nations must make significant efforts to address the problem from an interdependent stance, which means to:

A. Recognize (1) the transnational nature of the problem and (2) the essential role played by the *gatekeepers* of information highways (i.e. internet service providers) to investigate and prosecute cybercrimes; and
B. Strengthen the international framework (1) to establish more efficient mechanisms of transnational cooperation among nations and private actors, and, if possible, (2) to procure a greater uniformity among national legislations.

In the end, the solution seems to be "to adapt the constitutional framework of modern democracies" to the new electronic environment in which cybercrime thrives and in which governments, corporations and citizens interact and make democracies possible (Mecinas Montiel 2016, p. 427).

2.2 E-challenges to deliberative democracy

As mentioned before, new information technologies, specially the Internet and social media, have significantly changed what Habermas called the "public sphere". In contrast with the traditional mass media, the Internet has an open-ended multidirectional architecture, and the access costs are relatively low. These traits make the Internet a particularly effective media for common citizens to become active speakers instead of just receivers of information. This phenomenon has provoked not only an enormous diversification of accessible contents but has also modified the relative power of traditional mass media and has created a "networked information economy" (Benkler 2006, p. 212-213).

The Internet offers several tools (e-mail, blogs, writable web, hyper-text protocols, etc.) that allow individuals to become broadcasters themselves and create "conversational large-scale collaborative content" (Benkler 2006, p. 215-219). These technologies have enabled the emergence of "non-market actors" and the creation of a "networked public sphere" in which contents and influence are determined by the relations of all actors, instead of just by some (as

in the traditional mass media). In this "networked public sphere", individuals can "monitor and disrupt the use of mass media power" thanks to the immediate access to several sources of information and data distribution. Individuals or groups with "intense political engagement" can become press-like actors themselves but, unlike traditional mass media, their influence rely on a "see for yourself culture". These traits obviously facilitate the organization of collective political actions and foster the democratization of the "public sphere" (Benkler 2006, p. 220).

Some authors argue that, as long as the Internet remains an open-ended structure, the logic of the network economy will not allow excessive power concentrations, because the earnings come from getting the people's attention, and not from the pricing of Internet services (Benkler 2006, p. 240). However, others argue that the *architecture* and coding of the most relevant internet forums and browser might concentrate enormous power in private hands: the power to control information highways. According to authors such as Van Dijck (2013) and McChesney (2013), cultural norms and values affect the shape and functions of specific social media platforms and the whole ecosystem of social media, and in turn, the technological, ideological and socioeconomic structures of those ecosystems, through coding and commoditizing social relationships, are "profoundly altering the nature" of social interaction by feeding their users only the information akin to their interests and worldviews. Companies like Facebook or Google have so much capacity to code and commoditize online social interactions that they have practically become the *architects* of such ecosystems. Even though their activities are still roughly within legal boundaries, the high compartmentalization and concentration of power in few hands present critical governance, legislative and social issues, especially in relation to democracy.

Rights to the protection of personal data and privacy, freedom of commerce and electoral equity

Social media and search-engine companies can shape online social interactions not only because they have the power of coding the environments of such interactions, but also because of their capacity to profile ("profiling") and predict their user's attributes and behaviors. These companies can easily access "digital records of behavior, such as Facebook Likes, browsing histories, search queries, or purchase histories can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender" (Graepel *et al*. 2013). Furthermore, these *architects* can process such information to create highly accurate profiles of their users, predict their preferences, and even target them with individualized data and advertising in order to promote or discourage specific behaviors.[*]

These kinds of interventions pose a direct threat to electoral equity and a possible abusive use of personal data. On one side, companies like Facebook or Google commoditize their users' information and sell them in the market. Buyers, on the other side, use such information with little or no accountability to influence consumers and sometimes voters, through "tailored ads based on personal data" (Christopher Wylie, as quoted by Guimón 2018). That was exactly the case of Cambridge Analytica (CA), the company that is being investigated for its alleged role in the 2017 US presidential elections and in the Brexit referendum.[†]

---

[*] For instance, according to an account by Robert Epstein (2016):
"… a study by Robert M Bond, now a political science professor at Ohio State University and others, published in Nature in 2012, described an ethically questionable experiment in which, on election day in 2010, Facebook sent 'go out and vote' reminders to more than 60 million of its users. The reminders caused about 340,000 people to vote who otherwise would not have. Writing in the New Republic in 2014, Jonathan Zittrain, professor of international law at Harvard University, pointed out that, given the massive amount of information it has collected about its users, Facebook could easily send such messages only to people who support one particular party or candidate, and that doing so could easily flip a close election – with no one knowing that this has occurred. And because advertisements, like search rankings, are ephemeral, manipulating an election in this way would leave no paper trail."

[†] The Company profiled voters for Trump´s campaign by acquiring their Facebook information, influencing political preferences according to their personal interests. The deformation of the perception of voters without their knowledge infringe their free will to make a decision (Mccausland, P.

There are, at least, three sets of rights involved and colliding in cases like Cambridge Analytica (CA): personality rights (e.g. privacy and personal data protection); commercial rights (i.e. freedom of commerce); and political rights (electoral equity, right to information). The conflict between personality rights and political rights is not new: the undue use of the voters' registry data for electoral purposes or the excessive disclosure of a candidate's personal information in the heat of a political campaign are common scenarios of such conflicts. Most democracies would deem the first scenario as a clear violation of the right to privacy and a breach to electoral equity, even if political parties have the right to access such information. Whereas the nature of the democratic debate would allow for an extended permissiveness of the political right of expression over the candidate´s right to privacy, provided that those expressions do not clearly constitute defamation or slander (Electoral Tribunal of Mexico, d, e, f). Contemporary democracies are used to these scenarios and have produced a rather abundant set of rulings and national legislation on the matter (see Appendix B)

The conflict between personality and political rights, on the one hand, and rights of commerce on the other hand, are not so common, and their point of equilibrium in the era of the Internet and social media is not so clear. The collision between those sets of rights arises when private companies or even political parties use personal data to influence elections, without the explicit authorization of the affected individuals and in clear violation of electoral regulations.

In relation to personality rights, even if it is true that social media users must explicitly accept the general privacy conditions imposed by the social media companies, they have little or no control on who is authorized to "buy" their personal information, or to what uses should it be put. This situation undermines the fundamental right to privacy and personal data protection, because it curbs the user's capacity to impose limits on the use of his/her personal information (Davara 2003, p. 43-44). In the ruling 292/2000, the Constitutional Tribunal of Spain established that "the fundamental right to the protection of personal data… grants the incumbent with a set of powers to impose on third parties the duty to perform or refrain from performing specific behaviors… which grants the individuals with the power to decide over their data… [a useless power] if the incumbent has no knowledge of what information is in the hands of third parties, who are those parties, and to which use will the information be put." (As referred by Davara 2003).[*]

Regarding political rights, the use and abuse of personal data for electoral purposes, cloaked as freedom of commerce, might pose a serious threat to electoral equity at least in three aspects: first, because private actors might use such information to directly exert undue influence on the electoral competition; second, because internet and social media companies, arguing freedom of commerce, might restrict the access to such information according to their political preferences, hence granting an unwarranted advantage to some parties or candidates over others; and third, because the commoditization of personal data represents a challenge to the surveillance of money in political campaigns.

According to the Code of Good Practice on Electoral Matters adopted by the Venice Commission, electoral equity and specifically equality of opportunity "applies in particular to radio and television air-time, public funds and other forms of backing" and entails "a neutral attitude by state authorities, in particular with regard to: i. the election campaign; ii. coverage by the media, in particular by the publicly owned media; iii. public funding of parties and campaigns." However, the Code also states that "legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections" and that "the principle of equality of opportunity can, in certain cases, lead to a limitation of political party spending, especially on advertising" (Code of Good Practice in Electoral Matters 2002).

The risk to undermine the rights to privacy and electoral equity suggests a need to regulate the commercial rights of internet and social media companies. Nonetheless, the Internet remains a

---

and Schecter, A., 2018, BBC, 2018).

[*] Own translation.

low-cost, open-ended multidirectional architecture because it allows for the commoditization of personal information, such as the users' browsing history, interaction patterns and personal data (Benkler 2006). To completely forbid such commoditization would also hinder the development of the Internet and, consequently, the access to an apparently limitless source of political information and democratic action. As long as societies don't find new forms to finance the Internet, to impose excessive limits on the commoditization of personal information could curtail fundamental political rights such as freedom of expression and freedom to organize political action. But social media and the Internet are not (and should not be) a space located outside legal parameters (Electoral Tribunal of Mexico, g), hence the urge to find solutions to these conflicts of rights that allow for a reasonable protection of privacy, political and commercial rights.

Freedom of expression, freedom of commerce and discourse radicalization: the "search-engine effect" and the dissemination of fake news

Besides the evident threats to personality rights and the damage to electoral equity by the misuse of personal information, this new "networked public sphere" has two additional inconveniences for democracy: first, the fact that its powerful architecture is privately owned poses a threat to freedom of expression; and second, the commercial logic and incentives of the *architects* have weakened and radicalized democratic discourse.

Freedom of Expression is a fundamental right recognized in the American Declaration on the Rights and Duties of Man, the American Convention on Human Rights, the Universal Declaration of Human Rights, Resolution 59 (1) of the United Nations General Assembly, Resolution 104 adopted by the General Conference of the (UNESCO) and the International Covenant on Civil and Political Rights. Moreover, freedom of expression is a necessary condition for the existence of a democratic society.[*] The right to access cyberspace is a necessary condition for the full exercise of freedom of expression and, thus, for democracy. The Internet provides practically infinite information and allows for a borderless, multidirectional, large-scale, low-cost social interaction and data exchange. The paradox is that the same technologies that have enhanced the possibilities of expression, are the ones that curtail such possibilities.[†]

There are two aspects of the Internet that might pose different sets of threats to democracy. First, the risk of state intervention through excessive or inadequate regulation; and second, the

[*] As expressed by Emily B. Laidlaw (Laidlaw 2015, p. 19-21):
"Democracy has always been embodied in the practices of communication, and freedom of expression has consistently been identified by the courts as central to democracy. In Lingens v. Austria, the European Court of Human Rights (ECtHR) famously commented that freedom of expression 'is one of the essential foundations of a democratic society'…
Many states, such as Estonia, Finland, France, Greece and Spain, have legislatively recognized internet access as a fundamental right. In 2003, the Committee of Ministers of the Council of Europe adopted a Declaration affirming the importance of freedom of expression on the internet. Since 2010, we have seen a paradigm shift at an international level in the recognition of human rights in the cyberspace. Access to the internet as a fundamental right received the United Nations (UN) stamp of approval in a report by Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression… This was followed up in 2012 by the UN Human Rights Council passing a resolution affirming internet freedom as a basic human right, in particular the right to freedom of expression".

[†] Again, in the words of Laidlaw (2015, p. xi-xii):
"[T]he communication technologies that enable or disable participation in discourse online are privately owned…Thus, we inevitably rely on these companies to exercise the right to freedom of expression online, and they thereby become gatekeepers to our online experience…
Our reliance on these gatekeepers to exercise the right to free speech has had two effects. First, such gatekeepers have increasingly been the target of legal measures designed to capitalize on their capacity to regulate third-party conduct… Second, …speech regulation in cyberspace has largely been left to self-regulation, in much the same way that regulation of the internet in general has been light-touch…. The result is a system of private governance running alongside the law, without any of the human rights safeguards one normally expects of state-run systems, such as principles of accountability, predictability, accessibility, transparency and proportionality".

lack of reasonable safeguards for human rights. The *gatekeepers* (ISP) and *architects* of the Internet have garnered so much power with so little regulation, that they represent a temptation for political actors: to use that power for political control purposes through inadequate regulation or to simply use the reach of the "networked public sphere" to manipulate preferences through the dissemination of political information with bots and trolls (Quintana 2016). Unjustified state surveillance of private communications and the artificial creation of *trending topics* (whether false or true) directly curb the freedom of expression and hinder democratic dialogue. Furthermore, it represents a breach of the institutional neutrality mandated by the Code of Good Practice on Electoral Matters of the Venice Commission, and a direct violation to electoral equity. That is why any regulatory attempt on the Internet and social media must be accompanied by and thoroughly discussed with both private actors and representatives of the citizenry.

Regarding the second aspect pointed out by Laidlaw, the *architects* of the Internet decide, through coding practices based primarily on commercial interests, the content and audience of every online communication. As a consequence, they have privately shaped the online democratic discourse and have fostered (perhaps inadvertently) undesirable consequences such as electoral preferences manipulation, *epistemic bubbles, echo chambers* and *fake news*, and their lack of regulation have left the users with no legal recourse to protect their data and, most of all, their freedom of expression and democratic rights.

The manipulation of electoral preferences has been documented by Rob Epstein, a senior research psychologist at the American Institute of Behavioral Research and Technology and former editor-in-chief of Psychology Today. He has studied and measured what he has called the *Search Engine Manipulation Effect* (SEME), that is the influence that search engines rankings (specially Google for its predominance) have in voting preferences (Epstein 2016). According to a study ran by the author and Ronald E. Robertson in 2015, higher-ranked items connected with web pages that favor one candidate, have a dramatic impact on the opinions of undecided voters. This is, as the authors state, a major discovery, since the results were strong and consistent (Epstein and Robertson 2015).

In the paper they present evidence from five experiments in two countries, suggesting the power and robustness of the search engine manipulation effect. Specifically, they show that "(i) biased search rankings can shift the voting preferences of undecided voters by 20% or more, (ii) the shift can be much higher in some demographic groups, and (iii) such rankings can be masked so that people show no awareness of the manipulation." In India's 2014 Lok Sabha elections, a massive 99.5% of the respondents were not able to detect that they were being exposed to biased rankings. One of the crucial elements of this phenomenon is "that people trust its search results implicitly, assuming that the company's mysterious search algorithm is entirely objective and unbiased."

Their conclusion is categorical: "knowing the proportion of undecided voters in a population who have Internet access, along with the proportion of those voters who can be influenced using SEME, allows one to calculate the win margin below which SEME might be able to determine an election outcome" (Epstein and Robertson 2015). This power to manipulate electoral preferences through search engines is mainly held by one single company, Google, which processes the unconceivable amount of 40,000 searches per second (Google Search Statistics 2018). Epstein and Robertson assert that "[s]wing voters have always been the key to winning elections, and there has never been a more powerful, efficient or inexpensive way to sway them than SEME. So if Google favours one candidate in an election, its impact on undecided voters could easily decide the election's outcome." In this context, it is "even more disturbing" the fact that "the search-ranking business is entirely unregulated" (Epstein and Robertson 2015).

Whether this manipulation is intentional or not, the SEME entails two important consequences for democracy: the power to manipulate preferences could be used by private or public actors to affect electoral equity; and the fact that search-engine users are unaware of the criteria (coding) of the ranking mechanisms hinders their capacity to make fully informed decisions, and therefore to exert their freedom of expression.

The *Search Engine Manipulation Effect* is not exclusive of online search engines. Social media platforms are also governed by an underlying coding architecture that is not unbiased. Companies like Facebook, Twitter or Instagram are primarily motivated by commercial interests, and design their coding structure according to those interests and not necessarily in function of democratic principles. In this sense, the algorithms that govern social media foster a partial and sometimes illusory comprehension of politics and democracy, because they provide biased information that reflect the partial interests and behavior of their users (Van Dijck 2013; McChesney 2013).

This situation has created what Thi Nguyen calls *epistemic bubbles* and *echo chambers* (Nguyen 2018). The former is "an informational network from which relevant voices have been excluded by omission." It is the natural consequence of the algorithms that govern social media: they feed their users only with information that replicates the interests and worldviews of each social group and exclude any data that does not match this criterion. Therefore, *epistemic bubbles* promote a partial comprehension of political reality and hamper freedom of expression. Even more, *epistemic bubbles* foster the development of *echo chambers*, social structures "from which other relevant voices have been actively discredited." Nguyen asserts that "[a]n echo chamber doesn't destroy their members' interest in the truth; it merely manipulates whom they trust and changes whom they accept as trustworthy sources and institutions." In a certain sense, the architecture of social media also encourages parameters of trust based on the confirmation or detraction of self-beliefs instead of on objective data.

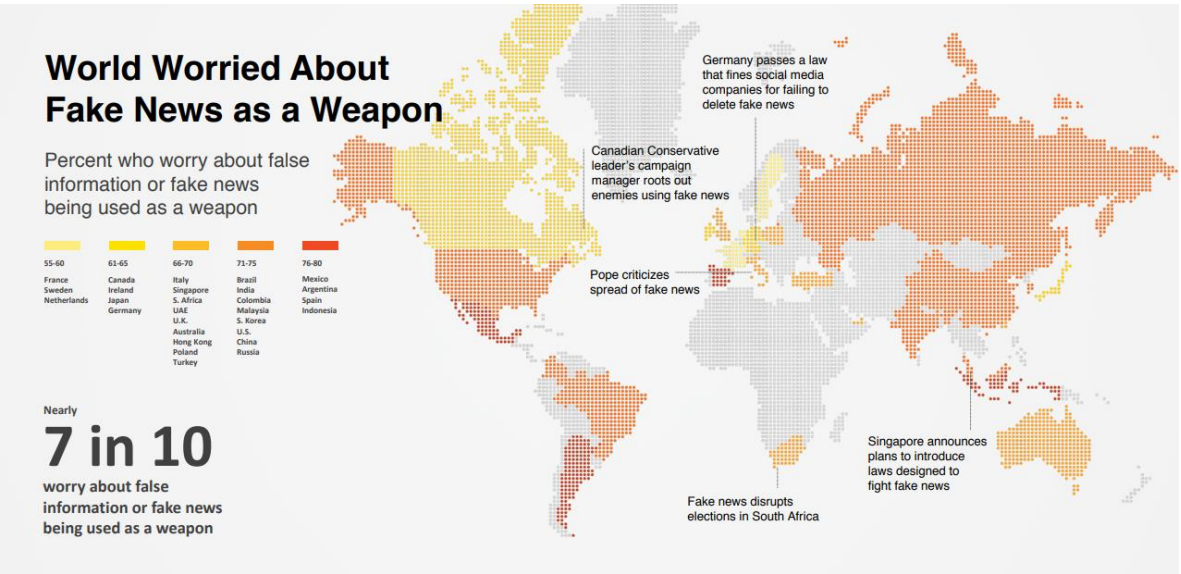
Epistemic bubbles and *echo chambers* have far reaching effects for democracy. First, the fact that trust parameters are based on subjective and extremely partial criteria pose a challenge for democratic legitimacy, because public institutions make decisions according to legal parameters that may or may not satisfy the strictly personal expectations of one social group or the other. Second, both "are social structures that systematically exclude sources of information… [and] exaggerate their members' confidence in their beliefs" (Nguyen 2018), hence undermining democratic dialogue. The "Internet poses a high risk of group polarization by the sole fact that facilitates the dialogue among individuals with similar opinions; which, ultimately, moves them to extreme and, in some cases, even violent positions" (Sunstein 2003, p. 181)[*]. And third, the fact that Internet and social media users can easily create "conversational large-scale collaborative content" (Benkler 2006), along with the biases caused by the *architects* of online social interaction (i.e. SEME, *epistemic bubbles* and *echo chambers*), foster que quick dissemination of information, sometimes disguised as news, without the rigorous fact-checking procedures of traditional media, usually known as *fake news*.

Fake news directly affect democracy. As explained before, biased and false information generate constitute an obstacle to an informed electorate, to the full exercise of freedom of expression and to the quality of democratic dialogue. And according to Freedom House, the manipulation and disinformation in social media played an important role in the elections of at least 18 countries during 2016, contributing to the decrease of freedom on the net and to physical and technical attacks against human rights defenders and independent media (Freedom House 2017).

The threat of *fake news* is not likely to decrease in the future. On the contrary, the increasing use of Internet and social media for political purposes will certainly expand their presence. According to the largest ever-made study of this phenomenon in digital media done by the MIT, *fake news* are more prone to circulate through digital means, where "[f]alsehood diffused significantly farther, faster, deeper, and more broadly than the truth […]", especially in political issues. The study tracked 126,000 stories on Twitter by roughly 3 million people from 2006 to 2017 and found that false claims were 70% more likely than the truth to be shared on Twitter; true stories were rarely retweeted by more than 1,000 people, but the top 1% false stories were shared by 1,000 to 100,000 people; and that it takes true stories about 6 times as long as false stories to reach people (Vosoughi, Roy and Aral, 2018). According to the Edelman Trust Barometer 2018 Global Report nearly 70% of the global internet users worry about *fake news*

[*] Own translation.

being used as a weapon:



Source: 2018 Edelman Trust Barometer. ATT_MED_AGR. Below is a list of statements. For each one, please rate how much you agree or disagree with that statement using a nine-point scale where one means "strongly disagree" and nine means "strongly agree". (Top 4 Box, Agree), question asked of half of the sample. General population, 28-market global total.

Fake news are not a novelty in the political or social realm. Disinformation has always been a strategy to discredit opponents and to sway political support to one side or the other. The real threat of *fake news* to democracy resides in four factors: first, their speed of dissemination through the internet; the fact that they are actually fostered by the current *architecture* of search-engines and social media; the lack of tools (either legal, social or technical) to identify them and stop their spread; and the difficult of investigating and prosecuting such online behavior. *Fake news* are but a symptom of a deeper problem: they are the consequence of the segmentation and magnifying effect of the Internet on social interactions. In this sense, to forbid the dissemination of *fake news* would represent just a legal palliative to the problem, besides the obvious difficulties of identifying the authors, gathering sufficient proofs and attributing responsibilities to online behaviors. The same reasoning applies to any regulation of the internet *architecture* to curtail its manipulative effects on democracy. To attend these questions, nations need the cooperation of both citizenry and internet corporations.

Like in the case of the threats to personality rights and the damage to electoral equity by the misuse of personal information on the Internet, there are three sets of rights involved and colliding in the case of the threats to freedom of expression by the privately owned *architecture* of the Internet: personality rights (i.e. freedom of expression); commercial rights (i.e. freedom of commerce); and political rights (right to information, freedom of expression and electoral equity). And much in the same way, excessive or inadequate regulation of the *architectural* aspects of the internet might be counterproductive. The commoditization of personal information that allows for a low-cost, open-ended multidirectional virtual space is possible precisely because of the current *architecture* of the Internet. Any attempt to regulate on this matter must consider the risk of hindering the accessibility and development of the Internet and, consequently, the freedom of expression and the democratic dialogue itself.

But then again, the problem should not be left unattended. The risk to undermine the rights to privacy by the misuse of personal information, and the damages to freedom of expression and electoral equity produced by the *architecture* of the Internet (i.e. *SEME*, *epistemic bubbles*, *echo chambers* and *fake news*), along with the lack of regulation that have left citizens with no efficient legal recourse to protect their personal and political rights, are situations that call for urgent action.

The common element of all the scenarios we have explored is that powerful private actors, motivated by primarily commercial interests, mediate the relation among citizens, their fundamental rights, and democracy. Those private actors have the power to hamper fundamental rights, while maintaining an essential platform for democracy, and must recognize

such responsibility. This “calls for a new system of human rights [and democratic] governance that takes account of private power yet is sensitive to the models of regulation that have emerged in the communications technology sector” [added concept] (Laidlaw 2015, p. xii-xiii). Furthermore, the “internet is the conduit for communication in the digital age, making it the heart of any system of free expression… The task in a dynamic and multinodal regulatory environment such as the internet is to link the various approaches to regulation in ways that are complementary, mutually reinforcing and responsive…” (Laidlaw 2015, p. 280-281).

In order to accomplish such goal, nations must work on a regulatory and adjudicatory approach different from the traditional top-bottom legal paradigm; a model that includes **co-responsibility** and **multiple regulatory and conflict-resolution approaches**. Such model might include at least **three strategies**, all of them able to constantly adapt to the ever-changing environment of the internet and communications technologies:

A. **Education** to strengthen legal and democratic culture of citizens;
B. **Self-regulation** like the mandatory adoption of ethics and corporate social responsibility codes; and,
C. **Remedial mechanisms** provided in laws, policies and alternate conflict resolution mechanisms.

CONCLUSIONS

The relationship between democracy and new technological environments is quite complex. On the one hand, the Internet and social media have become the dominant platform of political interaction in some democracies (Democracy Reporting International 2017); the use of those tools have strengthened the critical attitudes of citizens towards their governments (Gainous *et al.* 2016); some studies in Latin America even suggest that there exists a very high positive correlation (0.71) between the use of those online platforms and support to democracy as a desirable form of government (Basco 2018); and their widespread use facilitate the organization of large-scale social movements and a closer interaction between citizens and political parties (Castells 2011; Metaxas y Eni Mustafaraj 2012; Cohen et al. 2012; European Union 2015). On the other hand, the new virtual tools are used "[a]gainst elections… to suppress voter turnout, tamper with election results, and steal voter information… Against political parties and politicians... to conduct cyberespionage for the purposes of coercion and manipulation, and to publicly discredit individuals… [and] Against both traditional and social media… to spread disinformation and propaganda, and to shape the opinions of voters" (CSE 2017).

These cyberthreats to democracy are possible because this new digital realm allows for new forms of criminality and data commercialization that seriously threaten privacy rights, and modulates social interactions selectively (and sometimes strategically) feeding or hiding specific information to its users, thus fostering a partial understanding of reality and hampering freedom of expression. The fact that these social interactions take place in a virtual world does not mean that it has no effects on the material realm. As shown in this paper, the democratic dialogue is rapidly moving to virtual platforms, and online behaviors and information have enormous influence on voters' preferences, elections results and democratic governance. Hence, what is illegal in the material realm should also be in the digital world. The real challenge is to efficiently investigate and prosecute illegal online activities given the borderless nature of the Internet, and to effectively regulate the enormous power that *coding*, *profiling* and *commoditizing* of personal data, along with the lack of regulation, gives to the *architects* of the Internet, while preserving a harmonious balance among personality, commercial and political rights.

To address such a challenge, we must first recognize that the Internet and social media have completely reshaped the democratic landscape: there is **a new powerful player** in the equation, with its own interests and commercial rights that tend to collide with both personal rights (i.e. privacy, protection of personal data and freedom of expression) and political rights and principles (i.e. electoral equity). This change poses at least three challenges to democracies:

- The **ubiquity of the Internet: and its borderless nature** represent an obstacle to the investigation and prosecution of illegal online behavior and pose several legal challenges related to national sovereignty, the principle of territoriality, and access to remote data to constitute proofs and attribute responsibilities.
- The **private ownership of the information highways** in the hands of ISP, search engines and social media companies means that the democratic dialogue and access to relevant information is necessarily mediated by commercial interests. This situation has concentrated enormous power in private hands (sometimes wielded by governments) and have had a deep effect on democracies: from the illegal use of the Internet to tamper with democratic processes, steal voters' information and conduct cyberespionage, to the coding, profiling and commoditization of personal data to predict political preferences and target voters with partial information to promote or discourage specific behaviors.
- The **architecture of the Internet** has fostered, perhaps inadvertently, the radicalization of online political discourse and the weakening of the democratic "public sphere" through phenomena such as the *Search Engine Manipulation Effect, epistemic bubbles, echo chambers* and *fake news*.

To face these challenges, nations must make significant efforts to address the problem from an interdependent and global perspective, which means to:

A. Recognize (1) the transnational nature of the problem and (2) the essential role played by the *gatekeepers* and *architects* of information highways (i.e. internet service providers, and search-engine and social media companies) to investigate and prosecute cybercrimes;
B. Strengthen the international framework (1) to establish more efficient mechanisms of transnational cooperation among nations and private actors, and, if possible, (2) to procure a greater uniformity among national legislations.
C. Work on a regulatory and adjudicatory model based on the **co-responsibility** of private and public actors, and on **multiple regulatory and conflict-resolution approaches**. Such model might include at least **three strategies**, all of them able to constantly adapt to the ever-changing environment of the internet and communication technologies:
   - **Education** to strengthen legal and democratic culture among citizens;
   - **Self-regulation** like the mandatory adoption of ethics and corporate social responsibility codes; and
   - **Remedial mechanisms** provided in laws, policies and alternate conflict resolution mechanisms.

Furthermore, this new regulatory and adjudicatory model must be guided by general principles that allow for the inclusion of all affected public and private parties and the recognition of the shared responsibility of all, in order to guarantee a reasonable, harmonious yet effective solution. Such principles would be:

1) **Balance** among personality rights (freedom of expression, personal data protection and privacy), commercial rights (freedom of commerce) and social-political rights (electoral equity, democratic integrity).
2) **Co-responsibility.** Private actor *must* be a part of the solution.
3) **Adaptability.** Multiple regulatory approaches; and
4) **International cooperation.** Efficient information exchange mechanisms and, if possible, legislative homologation.

Just as technological development and adaptation are necessary conditions for the survival of human societies and individuals, so legal adaptation is essential for the subsistence of constitutional and democratic States. The Internet and new technologies have already become a vital component of contemporary democracies. Now, it is our responsibility, as representatives of democratic states and experts in constitutional democracies, to come up with solutions that ensure the necessary legal, economic and political conditions for both internet freedom and fair democracies to thrive and endure.

REFERENCES

The ACE Project, 2018, "E-Voting" available at http://aceproject.org/ace-en/focus/e-voting/countries. (Last visited: May 03, 2018).

Allcott, Hunt; Gentzkow, Matthew. 2017. "Social Media and Fake News in the 2016 Election," Journal of Economic Perspectives—Volume 31, Number 2—Spring 2017—Pages 211–236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf (Last visited: May 29, 2018).

American Declaration on the Rights and Duties of Man. Adopted by the Ninth International Conference of American States,Bogotá, Colombia, 1948. Available at: http://www.oas.org/en/iachr/mandate/Basics/declaration.asp (Last visited: May 29, 2018).

American Convention on Human Rights. Adopted at the Inter-American Specialized Conference on Human Rights, San José, Costa Rica, 22 November 1969. Available at: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm (Last visited: May 29, 2018).

Anderson, Ross. 2017. "The threat. A Conversation With Ross Anderson." Edge online magazine. May 8, 2017. Available at: https://www.edge.org/conversation/ross_anderson-the-threat (Last visited: May 29, 2018).

Asociación de Internet. 2018. "13° Estudio sobre los Hábitos de los Usuarios de Internet en México." Asociación de Internet. Available at: http://www.asociaciondeinternet.org.mx/es/estudios (Last visited: March 13, 2018]

Annan, Kofi. 2003. "The world information summit: Break the technology barrier." The New York Times, December 9, 2003. Available at: https://www.nytimes.com/2003/12/09/opinion/the-world-information-summit-break-the-technology-barrier.html . (Last visited: April 17, 2018).

Auchard, Eric; Bate, Felix. 2017. "French candidate Macron claims massive hack as emails leaked." Reuters. 6 May 2017. Available at: http://reuters.com/article/us-france-electionmacron-leaks-idUSKBN1812AZ (Last visited: May 29, 2017).

BBC News Staff. 2016. "Ghana Election Commission Website Hit by Cyber Attack." BBC News. 8 December 2016. Available at: http://www.bbc.com/news/world-africa-38247987 (Last visited: May 29, 2018).

Basco, Ana Inés. 2017. "Techno-integration of Latin America Institutions, exponential trade, and equality in the era of algorithms." Institute for the Integration of Latin America and the Caribbean. 2017. P. 110. Available at: http://bit.ly/2FsHYQm (Last visited: May 29, 2018).

Benkler, Yochai. 2006. "The wealth of networks: how social production transforms markets and freedom". New Haven [Conn.]: Yale University Press.

Córdova Vianello, Lorenzo. 2009. "Derecho y Poder". FCE. Mexico.

Bond, Robert *et al*. 2012. "A 61-million-person experiment in social influence and political mobilization," Nature 489, (2012), 295-298, Available at: https://www.nature.com/articles/nature11421 (Last visited: May 29, 2018).

Breuninger, Kevin; Mangan, Dan. 2018. "Trump can't block Twitter followers, federal judge says." CNBC. Published 1:04 PM ET Wed, 23 May 2018 . Available at: https://www.cnbc.com/2018/05/23/trump-cant-block-twitter-followers-federal-judge-says.html (Last visited: May 29, 2018).

Castells, Manuel. 2011. "Networks of Outrage and Hope." Cambridge, UK: Polity.

Canales, Katie. 2018. “Zuck and other Silicon Valley power players gathered in Paris to meet with French President Emmanuel Macron — here's who was there.” Business Insider. May 23th, 2018. Available at: http://www.businessinsider.com/emmanuel-macron-mark-zuckerberg-paris-2018-5 (Last visited: May 29, 2018).

Code of Good Practice in Electoral Matters, adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002). Available at: http://www.venice.coe.int/webforms/documents/CDL-AD(2002)023rev-e.aspx (Last visited: May 29, 2018).

Cohen, Cathy; Kahne, Joseph; Bowyer, Ben; Middaugh, Ellen; Rogowski, Jon. 2012. “Participatory Politics: New Media and Youth Political Action.” Available at: https://ypp.dmlcentral.net/sites/default/files/publications/Participatory_Politics_New_Media_and_Youth_Political_Action.2012.pdf (Last visited: May 29, 2018).

Coleman, Gabriella. 2012. “Coding Freedom: The Ethos and Aesthetics of Hacking.” Princeton University Press.

Compilation of Venice Commission opinions and reports concerning freedom of expression and media. 2016. Available at: http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)011-e (Last visited: May 29, 2018).

Convention on Cybercrime ETS No.185 (“Budapest Convention”) of the Committee of Ministers of the Council of Europe, adopted in its 109th Session on 8 November 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Last visited: May 16, 2018).

CSE. Communications Security Establishment of the Government of Canada. Cyber Threats to Canada's Democratic Process. Available at: https://www.cse-cst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf (Last visited: May 29, 2018).

Davara Rodríguez, Miguel Angel. 2003. “Anuario de derecho de las tecnologías de la información y las comunicaciones (TIC), 2003: trabajos doctrinales especializados, boletines de actualidad, reseñas de interés jurídico, glosario de términos, normativa y otras informaciones de interés.” Fundación Vodafone. Davara & Davara. Madrid. 717 p.

Davies, William. 2016. “The Age of Post-Truth Politics,” The New York Times, Aug. 24, 2016. Available at: https://www.nytimes.com/2016/08/24/opinion/campaign-stops/the-age-of-post-truth-politics.html (Last visited: May 29, 2018).

Democracy Reporting International. 2017. “Social media monitoring in elections,” Democracy Reporting International, diciembre 2017. Available at: http://democracy-reporting.org/wp-content/uploads/2018/02/Social-Media-Monitoring-in-Elections.pdf (Last visited: May 29, 2018).

Edelman Trust Barometer 2018 Global Report. Available at: https://bit.ly/2FtPgUV (Last visited: May 29, 2018).

Electoral Tribunal of Mexico. High Chamber of the Electoral Tribunal of the Federal Judiciary Branch of Mexico. Available at: http://187.141.6.45/siscon/gateway.dll?f=templates&fn=default.htm (Last visited: May 16, 2018).

a. Jurisprudence 17/2016.
b. Jurisprudence 18/2016.
c. Jurisprudence 19/2016.
d. SUP-RAP-192/2010 and 193/2010 and accrued,
e. SUP-RAP-194/2010
f. SUP-RAP-0119/2011.
g. SUP-REP-123/2017.

h. SUP-REP-95/2018.

Enfield, Nick. 2017. "We're in a post-truth world with eroding trust and accountability. It can't end well," The Guardian. Available at: https://www.theguardian.com/commentisfree/2017/nov/17/were-in-a-post-truth-world-with-eroding-trust-and-accountability-it-cant-end-well (Last visited: May 29, 2018).

Escritt, Thomas. 2017. "Dutch will hand count ballots due to hacking fears." Reuters. 1 February 2017. http://www.reuters.com/article/us-netherlands-election-cyberidUSKBN15G55A (Last visited: April 2017).

Epstein, Robert. 2016. "The new mind control." Aeon Magazine. Available at: https://bit.ly/1otOSfR (Last visited: May 29, 2018).

Epstein, Robert; Robertson, Ronald. 2015. "The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections," Proceeding of the National Academy of Sciences. Available at: http://www.pnas.org/content/pnas/112/33/E4512.full.pdf?with-ds=yes (Last visited: May 29, 2018).

European Court of Human Rights. 2012. Case number: 3111/10. Ahmet Yıldırım v. Turkey. Date of decision: December 18, 2012. Available at: https://globalfreedomofexpression.columbia.edu/cases/ahmed-yildirim-v-turkey/ (Last visited: May 29, 2018).

European Union. 2015. "Handbook for European Union Election observation," European External Action Service, September 2015. Available at: https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf (Last visited: May 29, 2018).

Fidler, David. 2017. "Transforming Election Cybersecurity," Council on Foreign Relations, May 17, 2017. Available at: https://www.cfr.org/report/transforming-election-cybersecurity (Last visited: May 29, 2018).

Fix Fierro, Héctor. 2005. "Los derechos políticos de los mexicanos. Un ensayo de sistematización." Edited by the Electoral Tribunal of the Federal Judicial Branch. México. 2005. pp.48. Collection: Notebooks about doctrinal aspects of the electoral justice. No. 8.

Flynn, D.J; Nyhan, Brendan and Reifler, Jason. "The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs about Politics", European Research Council.

Freedom House. 2017. Freedom on the Net: Manipulating Social Media to Undermine Democracy [online]. Freedom House. Available at: https://freedomhouse.org/report/freedom-net/freedom-net-2017 (Last visited: February 2018).

Fukuyama, Francis. 2017. "The Emergence of a Post-Fact World." Project Syndicate Jan 12, 2017. Available from: https://www.project-syndicate.org/onpoint/the-emergence-of-a-post-fact-world-by-francis-fukuyama-2017-01 (Last visited: April 04, 2018).

Gavara de Cara, Juan Carlos; de Miguel Bárcena, Josú; Capodiferro Cubero, Daniel. 2015. "El control judicial de los medios de comunicación". Bosch Editor. España.

Gainous, Jason *et al.* 2016. "Internet freedom and social media effects: democracy and citizen attitudes in Latin America," Online Information Review 40, 2 (2016), 712-738. Available at: http://www.emeraldinsight.com.ezproxy.sussex.ac.uk/doi/full/10.1108/OIR-11-2015-0351 (Last visited: May 29, 2018).

Ginsberg, David & Schrage, Eliot. "Facebook launches new initiative to Help Scholars Asses Social Media's Impact on Elections." Facebook Newsroom. 9th April 2018. Available at:

https://bit.ly/2v3vUVk (Last visited: May 29, 2018).

Global Digital Report 2018. Developed by We Are Social and Hootsuite. Available at: *https://digitalreport.wearesocial.com/* (Last visited: May 29, 2018).

Google Search Statics. Internet Live Stats. Checked on 18th April 2018. Available at: https://bit.ly/1rneFnz (Last visited: May 29, 2018).

Graepel, Thore; Kosinski, Michal & Stillwell, David. 2013. "Private traits and attributes are predictable from digital records of human behavior." 2013. Proceedings of the National Academy of Sciences of the United States of America. Available at: http://www.pnas.org/content/110/15/5802 (Last visited: May 29, 2018).

Guimón, Pablo. 2018. "Brexit wouldn't have happened without Cambridge Analytica." El País. 27th March. Available at: https://bit.ly/2q3dkXA (Last visited: May 29, 2018).

Habermas, Jürgen.

a. 1989. "Jürgen Habermas on society and politics: a reader." Boston: Beacon Press.
b. 1991. "The Public Sphere." In Rethinking popular culture: contemporary perspectives in cultural studies, edited by Michael Schudson, 512. Berkeley: University of California Press.
c. 1998. "Between facts and norms: contributions to a discourse theory of law and democracy" MIT press.

Informe Latinobarómetro 2017. Page 42. Available at: https://bit.ly/2pGKNtW (Last visited: May 29, 2018).

International Covenant on Civil and Political Rights. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966. Available at: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Last visited: May 29, 2018).

International IDEA. 2014. "Social Media: A Practical Guide for Electoral Management Bodies." Available at: https://www.idea.int/sites/default/files/publications/social-media-guide-for-electoral-management-bodies.pdf (Last visited: May 29, 2018).

Laidlaw, Emily B. 2015. "Regulating speech in cyberspace: gatekeepers, human rights and corporate responsibility." Cambridge, U. K.: Cambridge University Press, 330 p.

McChesney, Robert. 2013. "Digital Disconnect." New York: New Press.

Metaxas, Panagiotis; Mustafaraj, Eni. 2012. "Social Media and the Elections," Science magazine 26, 338 (2012), 472-473, http://science.sciencemag.org.ezproxy.sussex.ac.uk/content/338/6106/472 (Last visited: May 29, 2018).

Mong, Attila. 2017. "Countering fake news while safeguarding free speech", Deutsche Welle Akademie, 14 de marzo de 2017. Disponible en http://p.dw.com/p/2Z7pu (Last visited: May 29, 2018).

Mudde, Cass. 2018. "Why the hysteria around the 'fake news epidemic' is a distraction", The Guardian, 7 de febrero de 2018. Available at: https://www.theguardian.com/commentisfree/2018/feb/07/hysteria-fake-news-epidemic-distraction?CMP=share_btn_tw (Last visited: May 29, 2018).

Nakashima, Ellen. 2016. "Russian Hackers Targeted Arizona Election System." The Washington Post. 29 August 2016. https://www.washingtonpost.com/world/nationalsecurity/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-

b19e428a975e_story.html?utm_term=.76054fb28944 (Last visited: February 2017); and "Illinois Voter Registration System Records Breached." State Board of Elections. 31 August 2016. https://www.elections.il.gov/Downloads/AboutTheBoard/PDF/08_31_16PressRelease.pdf (Last visited: February 2017).

Nelson, Jacob. 2017. "Is "fake news" a fake problem", Columbia Journalism Review, January 31, 2017. Available at: https://www.cjr.org/analysis/fake-news-facebook-audience-drudge-breitbart-study.php (Last visited: May 29, 2018).

NGUYEN, Thi. "Escape the echo chamber." 2018. Aeon Magazine. Available at: https://bit.ly/2GLC163 (Last visited: May 29, 2018).

ODNI, Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." 6 January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf (Last visited: February 2017).

Pro Truth Pledge, https://www.protruthpledge.org/ (Last visited: May 29, 2018).

Quintana, Yolanda. 2016. "Ciberguerra." Madrid, España. Editorial Catarata.

Recio Gayo, Miguel (Coord.). 2016. "La Constitución en la sociedad y economía digitales: temas selectos de derecho digital mexicano." Ciudad de México: Suprema Corte de Justicia de la Nación, Centro de Estudios Constitucionales, 511 p.
a. Maqueo Ramírez, María Solange, "La libertad de expresión en el entorno digital. Retos frente a la privacidad," pp. 89-130.
b. Mecinas Montiel, "Cyber Warfare," pp. 403-432.

Reuters Institute Digital News Report 2017. Available at: https://bit.ly/2tSeHbL (Last visited: May 29, 2018).

Rousseau, Jean Jaques. (1762) 2001. "El Contrato Social." Mestas. Madrid.

Salt, Marcos. 2017. "Obtención de pruebas informáticas en extraña jurisdicción: los "conflictos" del principio de territorialidad en un mundo virtual sin fronteras," en Dupuy, Daniela; Kiefer, Mariana (Coord.). 2017. "Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recopilación de evidencia digital. Responsabilidad de los proveedores de servicios de Internet." Editorial IBdeF, Montevideo-Buenos Aires, pp. 517-546.

Sartori, Giovanni. 1998. "En defensa de la representación política." Conference in the Spanish Congress. Available at: https://bit.ly/2v6tdCe (Last visited: May 29, 2018).

Springall, Drew; Finkenauer, Travis; Durumeric, Zakir; Kitcat, Jason; Hursti; Harri; MacAlpine, Margaret; Halderman, J. Alex. 2014. "Security Analysis of the Estonian Internet Voting System," published in CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Pages 703-715, Scottsdale, Arizona, USA — November 03 - 07, 2014, ACM, New York, NY, USA, 2014.

Sunstein, Cass R. (tr. de Paula García Segura). 2003."Internet, democracia y libertad". Barcelona: Ediciones Paidós Ibérica, c2003. 212 p.

The Web Foundation (2014) The Web Index 2014-2015 [online]. The Web Foundation. Available at: http://thewebindex.org/ [Accessed Tuesday 13th March 2018]

Tarun Wadhwa, "Kenya's Election Proves Fake News Is A Serious Threat To International Security". Available at: https://www.huffingtonpost.com/entry/kenyas-election-proves-fake-news-is-a-serious-threat_us_59a5c0e0e4b05fa16286bdd1 (Last visited: April 4, 2018).

The Social Media Election 2017. Available at: https://www.demos.co.uk/project/the-social-media-election/ (Last visited: April 4, 2018).

Trust in Media 2018 Report. Developed by the European Broadcasting Union. Available at: https://bit.ly/2qlaT3z (Last visited: May 29, 2018).

United Nations.

a. Resolution 62/7 adopted by the General Assembly of the United Nations, in 8 November 2007. Support by the United Nations system of the efforts of Governments to promote and consolidate new or restored democracies. 2007. Available at: http://undocs.org/en/A/RES/62/7 (Last visited: May 29, 2018).
b. Resolution 59 (1) of the United Nations General Assembly.
c. Resolution 104 adopted by the General Conference of the (UNESCO)

Universal Declaration of Human Rights of the United Nations. 1948. Available at: http://www.un.org/en/universal-declaration-human-rights/ (Last visited: May 29, 2018).

Van Dijk, José. 2013. *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press.

Vosoughi, S., Roy, D. and Aral, S. 2018. “The spread of true and false news online”. Science, 359 (6380): 1146-1151. Available at: http://science.sciencemag.org/content/359/6380/1146 (Last visited: May 29, 2018).

World Wide Web Foundation. 2014. *Web Index 2014*. Available at: https://bit.ly/2be2d86 (Last visited: May 29, 2018).

APPENDIX A

THE USE OF SOCIAL MEDIA DURING ELECTORAL PROCESSES: A COMPARATIVE ANALYSIS OF NATIONAL LEGISLATION AND CASE-LAW*

INTRODUCTION

Globalisation and technology are rapidly changing the interaction between citizens, institutions, and the way politics work. As a result, democratic processes are also being transformed: electoral campaigns are encountering new arenas, and the dialogue between representatives and the people they represent is becoming more horizontal, thus forcing the evolution of institutions towards these new patterns. The objective of this research paper in to analyse the institutional and legal response to these new dynamics, specifically regarding the use of social media during electoral processes.

This analysis adopts a definition of social media as:

> "web or mobile-based platforms that allow for two-way interactions through user-generated content (UGC) and communication. Social media are therefore not media that originate only from one source or are broadcast from a static website. Rather, they are media on specific platforms designed to allow users to create ('generate') content and to interact with the information and its source (International IDEA 2014: 11).
>
> While social media rely on the internet as a medium, it is important to note that not all internet sites or platforms meet the definition of social media. Some websites make no provision for interactivity with the audience, while others allow users only to post comments as a reaction to particular published content as discussions posts (or 'threads') which are moderated and controlled" (International IDEA 2014: 11).

Therefore, social media are different from other types of media as they enable and encourage interaction between users; an interaction that moves rapidly, increasing the information flows within society. This creates new challenges for institutions: 1) how to adapt to these trends, from an institutional and legal perspective; and 2) how to take advantage of this to create a more fluid and constant dialogue with citizens, and thus strengthen democracy.

To address these questions, the analysis will focus on the actions that have been taken in order to face the outburst and adoption of social media during electoral campaigns. Through empirical examples, the study will tackle the question of whether regulation for social media in electoral contexts is desirable and/or required. This will facilitate an informed debate towards the adoption of guidelines on the topic.

SOCIAL MEDIA AND ELECTIONS: ITS RELATIONSHIP WITH VOTER TURNOUT

According to *Digital in 2017 Global Overview*,† half of the world's population now uses the internet, and the number of social media users grew by more than 20% over the past 12 months. There are by now 2.7 billion of "active social media users".

The countries with the largest number of active Facebook users are the United States (214 million), India (191 million), Brazil (122 million), Indonesia (106 million) and Mexico (76 million). According to this analysis, Twitter focuses, and will continue to do so, on moments in time, that is, the creation, experience and report on episodes occurring on real time. Facebook has also incorporated features to provide instant information for users through Facebook Live. These new mechanisms to maintain people constantly informed have imposed new forms of interaction and new necessities of real time information for citizens.

---

* This is a collaboratively updated version of the draft originally presented by Justice José Luis Vargas Valdez on June 15, 2017, at the 59th Meeting of the Council for Democratic Elections.

† *Digital in 2017 Global Overview*, https://es.slideshare.net/wearesocialsg/digital-in-2017-global-overview

Content published and shared in social media has a variety of authors: virtually, every person can publish something that can be shared and turn into a *trending topic*. This means that, during electoral campaigns, the control of the flow of information is compromised, and traditional media campaign regulation is defied.

But not all interactions on social networks are human. Programs known as "bots" produce automatized content on a large scale, and are able to create national, regional or even international trending topics, making it very difficult to identify the original author or even the veracity of the information they produce, in many occasions spreading "fake news". In the context of an election, such situations might prevent an accurate damage assessment and even establishing a liability attribution.

Moreover, the architecture of social media poses important restrictions on the flow, direction and concentration of information, fostering radical biases in the data that users see and share. Most social media create clusters of information that allow its users to see only the data within the cluster they belong to[*]. This phenomenon presents several questions about the actual effects that communications through social media might have on elections.

Under these circumstances, campaigners have the ability to micro-target political messages that increase the probability that parties and candidates campaign on wedge issues, that divide society but also have the ability to mobilize voters (Council of Europe, 2017). The long term effect of this strategy is the undermining of the political and social fabric of democracies and a perceived violations of voter's privacy.

But how does social media actually impact electoral turnout? According to the United Nations, there are 2.3 billion people aged between 15-34 years[†], and of the total users of Facebook (1.8 billion), 1.1 billion are aged between 18 and 43 years[‡]. These figures show that the number of users of social media represents 31% of the world population, and in most countries they are eligible voters. Furthermore, an increasing number of young people considers social media as a major source of news, for example according to the 8th Annual Asda'A Burson-Marsteller Arab Youth Survey 2016, showed that 45% of young people got informed through social media.

According to Shah (2015), "during India's 2014 election, the winning candidate, Narendra Modi, was the second most 'liked' politician on Facebook, trailing only US President Barack Obama"[§]. Even more, according to Castells (2011), social media on the Internet were essential for the social movements of the "Arab Spring" and, more recently, for the public demonstrations of Brazil, Turkey, Chile and Mexico[**].

These figures of social media users, public demonstrations and social movements, do not necessary mean a higher voter turnout. According to Sajuria (2016) the use of internet fosters direct and innovative forms of political participation, rather than traditional ones, such as voting

---

[*] According to authors such as Van Dijck (2013) and McChesney (2013), cultural norms and values (human connectedness) affect the shape and functions of specific social media platforms (microsystems) and the whole ecosystem of social (connective) media, and in turn, the technological, ideological and socioeconomic structures of those (micro/eco) systems, through coding and commoditizing social relationships, are "profoundly altering the nature" (normalization) of social interaction. Furthermore, the actual ecosystem of social media and the high compartmentalization and concentration of power in few hands (Facebook, Google, Apple) present critical governance, legislative and social issues. José Van Dijk. 2013. The Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press. And Robert McChesney. 2013. Digital Disconnect. New York: New Press.

[†] United Nations, Department of Economic and Social Affairs, Population Division (2015). World Population Prospects: The 2015 Revision, custom data acquired via website

[‡] *Digital in 2017 Global Overview*, https://es.slideshare.net/wearesocialsg/digital-in-2017-global-overview

[§] Seema Shah, "Guidelines for the Development of a Social Media Code of Conduct for Elections", *International IDEA*, 2015, p. 7.

[**] Manuel Castells. 2011. Networks of Outrage and Hope. Cambridge, UK: Polity.

to elect representatives[*].

There is an ongoing discussion about the ethics and effects of social media on the behaviour of individuals and the development of democratic societies. Hence the importance of addressing these issues from the perspective of the institutions responsible for the organisation and surveillance of electoral processes.

In addition, as the African Commission on Human and Peoples' Rights expressed in 2016, there were rising concerns with an "emerging practice of State Parties of interrupting or limiting access to telecommunication and messaging services, increasingly during elections"[†].

REGULATION: AN INSTITUTIONAL RESPONSE TO THE USE OF SOCIAL MEDIA?

Under this context, legislators, electoral management bodies and constitutional courts have to balance the necessity to create new electoral regulation that takes into account the use of social media during electoral processes. Nonetheless, this awakens a new tension: does regulation on the use of social media imposes a restriction on freedom of expression?

This question gains relevance as, according to internet companies, in the second half of 2016, content removal requests from court orders, law enforcements and executive branches of government from more than 100 countries in the world, reached record numbers[‡].

Freedom of Expression is "a fundamental right recognized in the American Declaration on the Rights and Duties of Man and the American Convention on Human Rights, the Universal Declaration of Human Rights, Resolution 59 (1) of the United Nations General Assembly, Resolution 104 adopted by the General Conference of the United Nations Educational, Scientific and Cultural Organization (UNESCO), the International Covenant on Civil and Political Rights, as well as in other international documents and national constitutions".[§] It establishes the right of every person to seek, receive and convey information and opinions freely, regardless of, among other things, political opinions. Therefore, any regulation that aims to limit the freedom of expression to any citizen can be considered against this fundamental right.

However, one of the five principles of democratic elections is *equity*, and specifically equality of opportunity. As pointed out in the Code of Good Practice on Electoral Matters adopted by the Venice Commission:

> a. *Equality of opportunity must be guaranteed for parties and candidates alike. This entails a neutral attitude by state authorities, in particular with regard to:*
> i. *the election campaign;*
> ii. *coverage by the media, in particular by the publicly owned media;*
> iii. *public funding of parties and campaigns.*
> b. *Depending on the subject matter, equality may be strict or proportional. If it is strict, political parties are treated on an equal footing irrespective of their current parliamentary strength or support among the electorate. If it is proportional, political parties must be treated according to the results achieved in the elections. Equality of opportunity applies in particular to radio and television air-time, public funds and other forms of backing.*
> c. *In conformity with freedom of expression, legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections.*

[*] Sajuria, J., "More Political, Less Voting: the Internet Paradox", in "More Sex, Lies and the Ballot Box" (eds. Rob Ford & Phil Cowley)

[†] 362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa. African Commission on Human and Peoples' Rights 2016.

[‡] World Trends in Freedom of Expression and Media Development. Global Report 2017/2018. UNESCO http://unesdoc.unesco.org/images/0026/002610/261065e.pdf

[§] Inter-American Commission on Human Rights, *Declaration of Principles on Freedom of Expression*, https://www.cidh.oas.org/Basicos/English/Basic21.Principles%20Freedom%20of%20Expression.htm

d. Political party, candidates and election campaign funding must be transparent.
e. The principle of equality of opportunity can, in certain cases, lead to a limitation of political party spending, especially on advertising.[*]

Regarding social media, there is a blurred distinction between advertising and citizen participation. Also, how political parties spend their resources can be difficult to track and, in some countries, even unlawful. Also, global companies such as Facebook and Twitter, have international headquarters and may be out of reach for national monitoring mechanisms. Political parties have incorporated these new information technologies to advance their interests, support their candidates and get more votes during elections. For example, according to The Guardian and The New York Times, 87 million Facebook profiles were harvested by Cambridge Analytica, which in turn used them to benefit candidates and election results in several countries.

The Guidelines on Political Party Regulation (Venice Commission, 2010) note that the control of political party funding is essential to guarantee political parties' independence from undue influence and to ensure the opportunity for all parties to compete in accordance with the principle of equal opportunity and to provide for transparency in political finance. Social media and the internet have made harder to ensure the latter, because of the big shifts of advertising from traditional media to digital outlets, and the need for new methods to track and calculate digital expenses.

Legislation and case-law on the matter has been drafted in several countries to face this tension between freedom of expression and equality of opportunity on electoral processes.

NATIONAL AND INTERNATIONAL LEGAL FRAMEWORKS AND CASE-LAW

As a relative new phenomenon, there are a few but increasing number of international documents that address the issue. As noted in the Joint Declaration on Freedom of Speech and Internet[†], the approaches to regulation developed for other means of communication – such as telephone services or broadcasting – are very different to the ones needed for the Internet, and such methods must be specifically designed for it (Joint Declaration on Freedom of Expression and the Internet, 2011).

The recent Joint Declaration now includes "Fake News", Disinformation and Propaganda[‡], and underlines the necessity to prioritize the freedom of speech, stating that the prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a)[§], and should be abolished.

International organizations have also contributed to this effort. For example, the International Institute for Democracy and Electoral Assistance (International IDEA) has developed a model code of conduct for the use of social media during elections aimed for electoral management bodies[**]. The European Court of Human Rights, as well as the Inter-American Court of Human Rights, have stated the importance of freedom of speech in a democratic

[*] *Code of Good Practice in Electoral Matters*, adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002).
[†] Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011.
[‡] Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 3 March 2017..
[§] States may only impose restrictions on the right to freedom of expression in accordance with the test for such restrictions under international law, namely that they be provided for by law, serve one of the legitimate interests recognised under international law, and be necessary and proportionate to protect that interest.
[**] Seema Shah, "Guidelines for the Development of a Social Media Code of Conduct for Elections", *International IDEA*, 2015.

society as a fundamental condition for the development and personal progress of each individual, with regard that it must guarantee not only the dissemination of favourable or inoffensive information or ideas, but as well those offensive, ungrateful or that disturb the State (Ivcher Bronstein vs Perú (2001) 153).

Examples of relevant national legislation

A first analysis of the existing regulations shows a wide range of possibilities for national legislation. For instance, the table in Appendix B presents examples of the existing regulation in countries that are members of the Venice Commission. They have been classified in three groups, based on specific references in the legislation to a) internet, b) social media and c) not specified (if the regulation suggests a reference to the previous two items, but the terms are not explicit).

Examples of relevant case-law

Decisions made by courts and other bodies regarding the use of social media in electoral processes also shed light on how freedom of expression and equality in the competition have been assessed in challenging contexts. Some of these decisions can also be consulted in Appendix B.

OTHER MECHANISMS
Special units

The creation of specialized units to combat *fake news*.

a) United Kingdom (to be set up): A national security communications unit to tackle fake news disinformation

b) Czech Republic: The Centre Against Terrorism and Hybrid Threats, part of the Interior Ministry, it is a specialized analytical and communications unit that monitors threats directly related to internal security, which implies a broad array of threats and potential incidents relative to terrorism, soft target attacks, security aspects of migration, extremism, public gatherings, violation of public order and different crimes, but also disinformation campaigns related to internal security. with proposals for substantive and legislative solutions that it also implements where possible. It also disseminates information and spread awareness about the given issues among the general and professional public.

Codes of Good Practice

There is an initiative to compile a set of written rules to explain how to tackle phenomena such as fake news and disinformation, which includes recommendations for social media and internet companies in order to comply with these rules.

a) The European Commission will create a Code of Practice with the aim of:
   - Ensuring transparency about sponsored content, in particular political advertising, as well as restricting targeting options for political advertising and reducing revenues for purveyors of disinformation;
   - Providing greater clarity about the functioning of algorithms and enabling third-party verification;
   - Making it easier for users to discover and access different news sources representing alternative viewpoints;
   - Introducing measures to identify and close fake accounts and to tackle the issue of automatic bots;
   - Enabling fact-checkers, researchers and public authorities to continuously monitor online disinformation;

The Code of Practice is expected to be launched in July, 2018.

Network of Fact-checkers

Network of people working together to fact-check online information.

a. The International Fact-Checking Network (IFCN) works as a unit of the Poynter Institute that is dedicated to bringing together fact-checkers worldwide. The IFCN was created in 2015, to support and study the work of 64 fact-checking organizations from around the globe.
b. The European Commission will create an independent European network of fact-checkers, that will be selected from the European members of the IFCN. The network will develop working methods, establish best practices, in order to achieve the broadest coverage for factual corrections. The Commission will give the network the online tools needed, a secure European online platform on disinformation, to help it achieve its goal.
c. #Verificado2018 is a group of journalists, civil society and academic partners that seeks to debunk viral misinformation, fact check politicians' claims and combat fake news for the electoral federal process in Mexico.

TOWARDS CONCLUSIONS

This analysis highlights the importance of systematising available knowledge on the relationship between an increasing use of social media and electoral processes, and on how the relevant authorities will address the challenges to effectively protect rights related to political participation and representation. Freedom of expression and the equality in electoral processes are at the core of democracy and the new dynamics of communication pose challenges to guarantee them. For instance, a high-level group of experts on fake news and online disinformation acknowledged this in its report to the European Commission, but they also advised to disregard simplistic solutions, as any form of censorship either public or private that should clearly be avoided, as well as the fragmentation of the Internet, or any harmful consequences for its technical functioning. In order to harmonize the interests of private companies, citizens and democratic practices, an equilibrium between freedom of expression, privacy, and equality in the electoral processes must be sought and attained.

APPENDIX B

This section describes relevant national and international legislation and case law, and briefly explains the legal conflict or legally recognized issue and the solution provided in each case.

INDEX

A. RELEVANT NATIONAL LEGISLATION

1. Internet

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
1	**Albania**	*Electoral Code*, 2012 Article 84. Only those electoral subjects registered for elections are entitled to broadcast political advertisements during the electoral period on private radio, television or audio-visual media, be they digital, cable, analogue, satellite or any other form or method of signal transmission.	Freedom of expression VS Equity of elections	Equity of elections
2	**Argentina**	*National Electoral Code*, 2016 Article 64 ter. - (...) Among other media, it is forbidden to advertising on internet in order to promote the recruitment of candidates for elective public charges, before 25 days prior to the election.	Freedom of expression VS Equity of elections	Equity of elections
3	**Armenia**	*Electoral Code*, 2011 Article 6. Publicity of Elections 2. Individual decisions of the Central Electoral Commission shall be posted on the website of the Central Electoral Commission on the day of adoption in case of national elections… Normative decisions of the Central Electoral Commission shall be posted on the website of the Central Electoral Commission (...) 4. Candidates, political parties (alliances of political parties) participating in elections under the proportional electoral system, may, in national elections and elections of the Yerevan Council of Aldermen, submit their campaign programs in the	Legal recognition of Internet as a tool to reinforce transparency of elections	N/A

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		electronic form prescribed by the Central Electoral Commission for the purpose of posting on the website of the Central Electoral Commission. *Electoral Code*, 2011 10. (…) After the information on the number of voters having participated in the voting is published, it shall be posted on the website of the Commission as per electoral precincts (…) 11. The Central Electoral Commission shall, no later than starting at 0:00 hours on the day following the voting, carry out the tabulation of voting results as per electoral precincts. The Central Electoral Commission shall complete the tabulation of the preliminary results of the voting and shall post the preliminary results of the election on the website of the Commission. *Election Code*, 2013	Legal recognition of Internet as a tool to reinforce certainty of elections	N/A
4	**Azerbaijan**	Article 109. Immediately after the Constituency Election Commission submits the protocols on voting results to the Central Election Commission, preliminary results of the elections (referendum) shall be published by the Central Election Commission as a schedule providing unified voting results of election constituencies. Such information may be placed on the website of the Central Election Commission. *Election Law*, 2006	Legal recognition of Internet as a tool to reinforce certainty of elections	N/A
5	**Bosnia and Herzegovina**	Article 7.3. Candidates and supporters of political parties, lists of independent candidates, and coalitions, as well as independent candidates and their supporters, and election administration officials or those otherwise hired in the election administration are not allowed to: (...) 7. use language which could provoke or incite someone to violence or spread hatred, or to publish or use pictures, symbols, audio and video recordings, SMS messages, Internet	Freedom of expression VS Security	Security

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		communications or any other materials that could have such effect. *Elections Law*, 2012		
6	**Brazil**	Article 57-A. It is permitted to display electoral publicity on the Internet, under the terms of this Law, after July 5 of the election year. The publication on a website of a story focused on the launch of candidacy for the position of President of the Republic by a given party does not constitute extemporaneous publicity. *Elections Law*, 2012	Freedom of expression VS Equity of elections	Freedom of expression
		The publicity of primaries via the Internet goes beyond the inner boundary of the party, and therefore compromises the surveillance of its reach by the Electoral Justice. *Elections Law*, 2012	Freedom of expression VS Equity of elections	Equity of elections
7	**Chile**	Article 57-B. Electoral publicity on the internet may be conducted in the following manners: I - in a candidate's website, provided that its electronic address is reported to the Electoral Justice and that it is hosted, directly or indirectly, in an internet service provider established in the country; I - in a party's or coalition's website, provided that its electronic address is reported to the Electoral Justice and that it is hosted, directly or indirectly, in an internet service provider established in the country; III - via electronic messages sent to addresses collected without payment by the candidate, party or coalition; IV - by means of blogs, social networks, instant messaging websites and other similar services whose content is generated or edited by candidates, parties or coalitions or by initiative of any natural person. *Law No. 19.884 about Transparency, Limit and Control of Electoral Expenditure*	Legal recognition of Internet and social media as a means of electoral propaganda	N/A
		Digitally electoral propaganda, are all the communications that through	Legal recognition of Internet and social media	N/A

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		media such as websites, social media, telephony and mail that go beyond the personal circle of contacts and that such services are hired. The electoral propaganda that is hired represents an electoral expense as disposed in article 2 of the Law No. 19.884	as means of electoral propaganda	
8	**Georgia**	*Organic Law. Election Code*, 2014 Article 51. Information support for carrying out pre-election campaign (…) 11. For the purposes of the present Law, public opinion poll shall satisfy the following requirements: d) it shall not constitute a means of manipulating with public opinion or fundraising and it shall not be conducted via telephone, post or/ and internet;	Freedom of expression VS Equity of elections	Equity of elections
9	**Japan**	*Public Offices Election Law*, 2016 Article 235-5. Those who communicate by displaying a name or identity that is against truth with the purpose of not winning, winning or by using a method such as postal service, telegraph, telephone, Internet, etc., shall be punished by imprisonment without work or a fine of not more than 300,000 yen.	Freedom of expression VS Equity of elections	Equity of elections
10	**Kazakhstan**	*Constitutional Law on elections*, 2007 Article 12. Authorities of the Central Election Commission of the Republic of Kazakhstan 16-1) place on the official website (Internet- resource) of the Central Election Commission the legal acts on the election legislation, information on the appointment and conduct elections as well as on the results of vote count at the elections; *Public Official Election Act*, 2014 Article 8 (Responsibilities of Press for Fair Reports)	Legal recognition of Internet as a tool to reinforce transparency of elections	N/A

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
11	**South Korea**	Where a person who manages and controls broadcasting, a newspaper, wire service, magazine or other publications, a person who edits, gathers data, writes or reports, or any Internet press agency provided for in the provisions of Article 8-5 (1) reports or comments on the platform or policy of a political party, political views or other matters of a candidate (including a person who intends to be a candidate; hereafter the same shall apply in this Article) and broadcasts or reports the interview or discussion in which a representative of a political party, a candidate or his/her proxy participates, he/she or it shall be fair. *Constitutional law on Presidential and Jogorku Kenesh Elections*, 2015	Freedom of expression VS Equity of elections	Equity of elections
12	**Kyrgyzstan**	Article 39. Publishing of voting results. Voting returns at each election precinct and territory covered by the activities of the election commission, election results on the electoral constituencies in the volume of the data contained in the Protocols of the CEC and subordinate election commissions, shall be provided to voters, candidates, representatives of candidates and political parties, observers, international observers, representatives of mass media upon request. Voting returns for each election precinct shall immediately be placed on the official website of the CEC on a rolling basis. The voting return data placed on the official website of the CEC is the preliminary information of no legal significance. *Federal Law on the election of the President*, 2003	Legal recognition of Internet as a tool to reinforce certainty of elections	N/A
13	**Russia**	Article 46. Informing of voters 7. On the voting day, before the end of voting, no information about the voting results, the results of the election of the President of the Russian Federation shall be published (made public) and no such information shall be placed in information-telecommunications networks with unrestricted access	Freedom of expression VS Certainty of elections	Certainty of elections

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		(including the Internet). *Electoral Code*, 2015		
14	**The former Yugoslav Republic of Macedonia**	Article 69-a (1) As an election campaign is considered: public gathering and other public events organised by the campaign organiser, public display of posters, video presentations in public areas, electoral media and internet presentation, dissemination of printed materials and public presentation of confirmed candidates by official electoral bodies and their programmes. *Electoral Code*, 2016	Legal recognition of Internet as a mean of electoral propaganda	N/A
15	**France**	Article L52-1 During the six months preceding the first day of the month of an election and until the date of the ballot in which it is vested, the use for electoral propaganda purposes of any commercial advertising process by means of the press or by any means of audiovisual communication is prohibited. *Regulations on The Elections To The Chamber of Deputies and The Senate*, 2008	Freedom of expression VS Equity of elections	Equity of elections
16	**Romania**	Art. 37. – (1) During the electoral campaign, the candidates, political parties, political alliances, electoral alliances, organisations of citizens belonging to national minorities, as well as the citizens with a right to vote, shall be entitled to express their opinions freely and without any discrimination, by protests, gatherings, use of television, radio, written press, electronic means and of the other means of mass information. *Representation of the People Institutional Act*, 2015	Freedom of expression VS Equity of elections	Freedom of expression
17	**Spain**	Section 53. Notwithstanding the foregoing, from the call of the election to the legal start of the campaign, no commercial publicity or propaganda shall be allowed by means of posters, commercial supporting devices or advertisements in the press, in	Freedom of expression VS Equity of elections	Equity of elections

RELEVANT NATIONAL LEGISLATION - INTERNET				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		wireless station or digital means, nor can such acts be justified as the exercise of the ordinary activities of the parties, federations or coalitions acknowledged in the preceding subsection. *Organic Law on Elections and Referenda*, 2014		
18	**Tunisia**	Article 68. Principles of electoral campaigns fully apply to all electronic media and to all messages directed at the public via electronic means for the purpose of propaganda in the context of elections or referendums. The same principles apply to official websites of audiovisual communication enterprises, subject to the monitoring of HAICA.	Legal recognition of *electronic media* as a mean of electoral propaganda	N/A

2. Social media

RELEVANT NATIONAL LEGISLATION – SOCIAL MEDIA				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		Elections Law, 2012		
1	**Brazil**	Article 57-A. (…) Messages broadcast in Twitter during embargoed periods that lead to general knowledge of a future candidacy, political action or reasons that allow one to infer that its beneficiary is the fittest for the public office shall constitute extemporaneous publicity. The fact that it depends on the willingness of the Internet user to access the message contained in any a website does not preclude the possibility of characterizing extemporaneous publicity. *Electoral Code,* 2017 15. "Media service" shall be the creation and distribution of information	Freedom of expression VS Equity of elections	Equity of elections

RELEVANT NATIONAL LEGISLATION – SOCIAL MEDIA				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
2	**Bulgaria**	and content which are intended for reception by, and which could have a clear impact on, a significant proportion of the general public, irrespective of the means and technology used for delivery of the said information and content. The following shall be media services: (a) the print media (…) (b) the media distributed over electronic communications networks, such as: (aa) the public-service and commercial electronic media (…) providers of audiovisual media services or radio services; (bb) the online news-services (…) The social networks: Facebook, Twitter and other such, and the personal blogs shall not be media services.	Social networks NOT legally recognized as *Media Service*	N/A
3	**Chile**	*Law No. 18.700 about Popular Votes and Scrutinies* All content that is shared through personal social media and that it does not imply a hiring and payment of these services, will be considered private communications and therefore will not constitute electoral propaganda as specified in article 30 of the Law No. 18.700.	Freedom of expression VS Equity of elections	Freedom of expression
4	**Germany**	*NetzDG Network Enforcement Law* Social media companies and other providers that host third-party content to fines of up to €50 million if they fail to remove “obviously illegal” speech within 24 hours of it being	Freedom of commerce, freedom of expression VS	Equity of elections, security, honor

RELEVANT NATIONAL LEGISLATION – SOCIAL MEDIA				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		reported. – The law is described as applying to social media companies, but it defines that term very broadly, to include all profit-making internet platforms that are intended to allow users to share content with other users or make it publicly available. – The law also exempts providers who have fewer than 2 million registered users in Germany.	Equity of elections, security, honor	
		Political Parties, Elections and Referendums Act 2000 (PPERA), and the Representation of the People Act 1983. Under sections 85(3) and (4) of PPERA		
5	**United Kingdom**	In the UK, the use of election materials (i.e. election advertisements) by candidates and political parties in parliamentary and local elections are regulated under the Political Parties, Elections and Referendums Act 2000 ("PPERA") and the Representation of the People Act 1983. Under sections 85(3) and (4) of PPERA, election material is defined as material which can reasonably be regarded as intended to promote, procure or prejudice the success for political parties or candidates in elections. These include advertising posted by candidates and political parties on websites or YouTube videos created for dissemination. Under	Legal recognition of Internet and social media as a means of electoral propaganda	N/A

RELEVANT NATIONAL LEGISLATION – SOCIAL MEDIA				
#	Country	Law extract	Legal conflict or legally recognized issue	Legislating in favor of…
		the guidelines issued by the Electoral Commission, materials published on social media are regarded as election materials if they meet the criteria of a public test and a purpose test. For candidates and political parties, spending on social media is counted towards their applicable spending limit and must be reported in their returns on election expenditure. The spending include the design and production costs, cost related to updating the social media, and production of on-line petitions, and promotion cost from adding links to other websites.		

B. RELEVANT PROPOSED NEW LEGISLATION

1. Internet and social media

RELEVANT PROPOSED NEW LEGISLATION – INTERNET AND SOCIAL MEDIA				
#	Country	Proposed legislation summary	Legal conflict	Legislating in favor of…
1	**France**	*Bill to combat fake news* The proposed legislation to combat fake news was presented on March 21st, 2018. It is the result of the recent elections, which have demonstrated the existence of massive campaigns in order to disseminate fake information aimed to modify the electoral result. This bill has as an objective to thwart any destabilization operation that may occur during the upcoming elections in France, the reforms in the bill are in three specific areas: – First, the reforms seek to improve the fight against the dissemination of fake news during the electoral period, as of the publication of the decree that call the elections. – Secondly, the reforms aim to impose more transparency obligations to social media providers to make it easier for authorities to detect possible destabilization campaigns by external institutions by	Freedom of expression VS Equity of elections	Equity of elections

RELEVANT PROPOSED NEW LEGISLATION – INTERNET AND SOCIAL MEDIA				
#	Country	Proposed legislation summary	Legal conflict	Legislating in favor of…
		spreading fake news, and to allow users to know the nature of the providers that are advertised on the network. – Lastly, the reforms aim to allow the authorities to act expeditiously. *Honest Ads Act* Television and radio have long been required to disclose the purchasers and content of all who purchase advertisements on their stations. Internet companies have not.	Equity of elections	
2	**United States**	The Honest Ads Act, would mandate that internet companies reveal the identities and content of advertisements related to elections or campaigns. Specifically, this would be done by amending a decades-old existing campaign finance law from 1971, by adding the phrase "paid internet or paid digital communication" to its list of media forms subject to the law. It would also require any website with at least 50 million monthly viewers—including Facebook, Google, and Twitter—to maintain a public list of any organization or person who spends at least $500 in election-	VS Right to privacy / Freedom of commerce	Equity of elections

RELEVANT PROPOSED NEW LEGISLATION – INTERNET AND SOCIAL MEDIA				
#	Country	Proposed legislation summary	Legal conflict	Legislating in favor of…
		related ads. An exemption is made for "news story, commentary, or editorial" to ensure that the requirements are not levied on legitimate news reporting or opinion pieces.		

C. RELEVANT INTERNATIONAL LEGISLATION

1. Internet and social media

RELEVANT INTERNATIONAL LEGISLATION – INTERNET AND SOCIAL MEDIA			
#	Entity	Legislation Summary	Legally recognized issue
1	**European Union**	The General Data Protection Regulation (GDPR), will mark a turning point in the legislative framework for the use and protection of personal data in European Union (EU) countries. The GDPR will apply to every organization, that has clients in the EU, even if it has no establishment in it. The GDPR's provisions are mandatory and grant individuals numerous rights, including those to transparent communication, erasure (the right to be forgotten), and data portability (i.e., transfer from one data controller to another). These rights may be exercised and enforced not only by individuals but by organizations acting on behalf of individuals. Takes effect on May 25, 2018.	Legal recognition of the right to be forgotten and the right of data portability

D. RELEVANT CASE LAW

1. Internet

RELEVANT CASE LAW - INTERNET				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
1	**USA** District Court for the District of Columbia	*Shays v. FEC. 337 F. Supp. 2d 28 (D.C. 2004)* In relation with the 2002 Federal Election Commission Regulations on Internet Communications, the court found that the exclusion of Internet communications of the meaning of political communication in the Campaign Finance Statute, would prolong the current "soft money" system. *Unknown* (2008)	Freedom of expression VS Equity of elections	Equity of elections
2	**Brazil** Rio de Janeiro Regional Electoral Court	Pedro Dória and other bloggers posted messages and banners on their website of their wish that Fernando Gabeira would run for mayor of Rio de Janeiro. Since these messages were posted before the start of the three months campaign period, the Court ruled that the banners must be taken down. Nevertheless, afterwards the Court launched an ordinance allowing the publication of election campaign material on blogs. *Bland v. Roberts, No. 12-1671* (2013)	Freedom of expression VS Equity of elections	Equity of elections
3	**USA** Court of Appeals for the Fourth Circuit	Six employees of the Hampton, Virginia, Sheriff's Department brought suit against the Sheriff, alleging that he did not reappointment them due to their endorsement of his opponent's campaign in the 2009 elections. The support included clicking "Like" on the opponent's Facebook page. The Court held that clicking the "Like" button on the opponent's Facebook page constituted free speech and that three employees were terminated because of their respective support for the opponent, therefore ordering their reinstatement. *Case I ACa 1273/11* (2012)	Freedom of expression VS Institutional efficiency	Freedom of expression
		Andrzej Jezior was fined by the District Court in Tarnów (I Ns	Freedom of	

RELEVANT CASE LAW - INTERNET				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
4	**Poland** Krakow Court of Appeal	162/10) after some readers of his personal website posted negative comments regarding Bernard Karasiewicz, who was at the time the mayor of the town of Ryglice. The Krakow Court of Appeal reversed the judgment, establishing that Mr Jezior should not be held liable for the comments that appeared on his website.	expression VS Legal certainty	Legal certainty
5	**Singapore** Supreme Court of Singapore	*Lee Hsien Loong v. Roy Ngerng Yi Ling, SGHC 230* (2014) Roy Ngerng, a blogger, was found guilty of defamation for a blogpost in which he claimed that the Prime Minister of Singapore, Lee Hsien Loong, had criminally misappropriated contributions paid by citizens to a state-administered pension fund. Even though the plaintiff was a public figure and the defendant was discussing a matter of public concern, the Court found that the blogpost was malicious and undermined the credibility of the Prime Minister, and therefore determined that the right to sue for defamation overruled the defendant's right to freedom of speech.	Freedom of expression VS Honor	Honor
6	**European Union (France)** European Court of Human Rights	Plessis-Casso v. France, 34400/10 (2014) Henry de Lesquen du Plessis-Casso, Councillor of Versailles, posted an open letter on the Internet, accusing the deputy mayor of Versailles, "E.P.," of having intentionally waited to request French nationality in order to avoid serving in the military during the Algerian war. The Versailles Court of Appeals found Plessis-Casso guilty of defamation, whereby Plessis-Casso appealed his case before the European Court as a violation of the freedom of expression. The Court confirmed the ruling, arguing that although the issue was of general interest, Plessis-Casso attacked an aspect of the private life of E.P. and made statements that were not based on a	Freedom of expression VS Honor/ Right to privacy	Honor/ Right to privacy

RELEVANT CASE LAW - INTERNET				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
		sufficiently factual basis. *YouTube Corp. v. The Presidency of Telecommunication and Communication*, *2014/4705* (2014)		
7	**Turkey** Constitutional Court of Turkey	The Turkish Presidency of Telecommunication and Communication blocked YouTube after recordings of discussions between government officials had been posted on the website, arguing that it was necessary for national security interests. The Court found that the blockage of the entire website was unconstitutional and violated the freedom of expression. *Galloway v Frazer, Google Inc t/a YouTube and others*, *HOR9793* (2016)	Freedom of expression VS Security	Freedom of expression
8	**United Kingdom** High Court of Northern Ireland	George Galloway, a British Member of Parliament, brought suit against several YouTube videos posted by William Frazer, a political activist from Northern Ireland. He also brought legal action against Google Inc., the owner of YouTube, for failing to remove the videos expeditiously. The Court found that, in keeping one of the videos online for three weeks, Google failed to act sufficiently swiftly given the serious and alarming nature of the libel. Therefore, considering that the video was arguably defamatory, violated data protection law and constituted harassment, the Court allowed Galloway to serve proceedings outside of the jurisdiction on Google Inc. *2007 Hun-Ma1001* (2011)	Freedom of expression, Freedom of commerce VS Honor, Protection of personal data	Honor, Protection of personal data
9	**South Korea** Constitutional Court of South Korea	The Court determined that Article 93(1) of the Public Official Election Act, which prohibited the transmission of any information (including on the Internet) relating to a political candidate within 180 days of an election day, was unconstitutional. Although it found that its purpose to prevent corruption and to ensure fair	Freedom of expression VS Equity of elections	Freedom of expression

RELEVANT CASE LAW - INTERNET				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
		elections was legitimate, the Court found that the all-out ban was excessive and that the interests of democracy outweighed the purpose of the ban. *R v Bryan, 2007 SCC 12* (2007)		
10	**Canada** Supreme Court of Canada	Paul Bryan posted election results of the 2000 federal elections on his website to deliberately protest against Section 329 of the Elections Act prohibiting the reporting of election results until after the closing of all polling booths. The Supreme Court ruled that section 329 of the Elections Act was constitutional and that it also covered the Internet and blogs. The prohibition of banning the early posting of elections results was later repealed by the parliament. *Doe v. Cahill, 884 A.2d 451* (2005)	Freedom of expression VS Certainty of elections	Certainty of elections
11	**USA** Delaware Supreme Court	City councilman Cahill filed suit against defamation and invasion of privacy of an anonymous person, writing under the pseudonym “Proud Citizen” on a website devote to the discussion of local politics. The Delaware Supreme Court determined that, in order to protect the anonymous speakers’ First Amendment rights, plaintiffs must meet a “summary judgment standard” before piercing a defendant’s anonymity. This ruling permitted the anonymous person to remain anonymous. *Hadley v. Subscriber Doe, 34 N.E.3d 549* (2015)	Honor/ Right to privacy VS Freedom of expression, Anonymous speech	Freedom of expression, Anonymous speech
12	**USA** Supreme Court of Illinois	Freeport Journal Standard reader “Fuboy” commented on an online publication of the Standard’s article about local county board candidate Bill Hadley, comparing him to child molester “Sandusky” and noting that Hadley’s residence was adjacent to an elementary school. The Court determined that the comment was defamatory and that Comcast, Fuboy’s service provider, was required to release Fuboy’s identity.	Honor VS Freedom of expression, Anonymous speech	Honor

2. Social Media

#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
		REC na RP 182524 (2012)		
	Brazil		Freedom of expression	
1	Superior Electoral Court of Brazil	Indio da Costa, candidate for the Vice-Presidency of the Republic, on July 4, 2010, posted a tweet promoting José Serra, the candidate for President on his ticket. Since the tweet was posted two days before the start of the campaign period, the Court found that it constituted illegal electoral propaganda and fined Indio da Costa.	VS	Equity of elections
		SUP-RAP-268/2012 (2012)	Equity of elections	
	Mexico	Presidential candidate Andrés Manuel López Obrador, before the beginning of the electoral campaign period in 2012, published a tweet on his personal account with a link to a YouTube video of an interview he gave. The High Chamber found that the tweet did not constitute a premature campaign activity but rather an example of free expression on issues of national interest, considering that the video would only be viewed by a limited audience with Internet access and interested in political information.	Freedom of expression	
2	High Chamber of the Federal Electoral Tribunal	*Unknown* (2016)	VS	Freedom of expression
			Equity of elections	
		Sources: http://ewn.co.za/2016/07/30/EFF-welcomes-decision-by-Electoral-court-to-disqualify-its-candidate		
	South Africa		Freedom of expression	
3		And		Security
	Electoral Court of South Africa		VS	
		http://www.news24.com/elections/news/iec-acted-quickly-because-complaint-involved-whites-eff-20160729	Security	
		Thabo Mabotja was a candidate for councilor in Ward 7 in Tshwane when he posted a statement on Facebook, in which he called for white people to be "hacked and killed". The court ruled that the statement constituted a breach of the Electoral Code of Conduct in relation to the Promotion of Equality and Prevention of Unfair Discrimination Act and, therefore, disqualified him.		
		SUP-JRC-168/2016 (2016)		
	Mexico	Miguel Ángel Yunes Linares, pre-candidate for Governor of the state of	Freedom of	

RELEVANT CASE LAW – SOCIAL MEDIA				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
4	High Chamber of the Federal Electoral Tribunal	Veracruz, posted videos on Facebook as part of his campaign to become the official candidate of the political party PAN. The High Chamber found that these videos did not constitute premature campaign activities since they clearly identified Yunes Linares as a pre-candidate, did not request viewers to vote for him, and included criticisms of topics of general interest. The Tribunal stated that the publication of personal opinions on such topics on social media benefits from an assumption of spontaneity. *0382-E8-2018* (2018)	expression VS Equity of elections	Freedom of expression
5	**Costa Rica** Supreme Court of Costa Rica	Individuals, companies, profiles or pages on social media that broadcast polls or electoral surveys, without having been authorized to do so by the electoral institution, will be subject to a fine ranging from ten to fifty basic wages. *Public Ministry v. Castel-Branco and Mbanze* (2015)	Freedom of expression VS Equity of elections	Equity of elections
6	**Mozambique** District Court of Kampfumo	Carlos Nuno Castel-Branco, a renowned economist, posted a public letter on Facebook criticizing the President of Mozambique, Armando Emílio Guebuza, accusing him of corruption and comparing him to various dictators. The Public Ministry of Kampfumo charged Mr. Castel-Branco with slander and libel. The Court dismissed the charges, considering the post as healthy engagement in a democratic society and finding that Castel-Branco's right to freedom of expression trumped the President's right to privacy and the protection of his reputation.	Freedom of expression VS Honor / Right to privacy	Freedom of expression
7	**Brazil** Brazilian Supreme Court	*Lula v. Caiado I*, 4.088 (2015) and *Lula v. Caiado II*, 4.097 (2015) Senator Ronaldo Caiado posted statements accusing Luiz Inácio Lula da Silva, the former President of Brazil, of being a "bandit" who promoted democratic instability and of having committed crimes such as embezzlement and money laundering. Former President Lula charged Senator Ronaldo Caiado with libel and slander, but the Court dismissed the complaint based on parliamentary immunity. *Unknown* (2016)	Freedom of expression, State's stability VS Honor	Freedom of expression, State's stability

RELEVANT CASE LAW – SOCIAL MEDIA				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
	Turkey	Source: https://www.unian.info/world/1696296-10000-social-media-users-currently-under-investigation-in-turkey.html	Freedom of expression	
8	First Instance Court in Istanbul	Model and former Miss Turkey, Merve Buyuksarac, was handed down a 14 month suspended prison sentence for insulting the Turkish president, Recep Tayyip Erdoğan. In 2014 she shared a poem on Instagram which did not refer to Erdoğan by name but alluded to the corruption scandal involving his family. *SM-JIN-35/2015*	VS Honor, Right to privacy	Honor, Right to privacy
	Mexico	On the Election Day, the Governor of the state of Aguascalientes used a government bus to travel to different polling stations with various candidates for federal representatives, posting pictures throughout the day on his Twitter account. This Twitter account was promoted on the official webpage of the Government of Aguascalientes. The Regional chamber annulled the election, considering that the Governor violated the principles of equality and impartiality, taking into consideration that the online publication of this information ensured that his involvement was well-known by the general public.	Freedom of expression	
9	Monterrey Regional Chamber of the Federal Electoral Tribunal		VS Equity of elections	Equity of elections
	Mexico	During the election silence, various famous Mexican personalities published tweets in favour of the Green Party (PVEM). Considering the number of tweets and the fact that they used the same positive references to the Green Party's candidates and proposals, the High Chamber found that the tweets were not an authentic exercise of the freedom of expression but rather part of the Green Party's propaganda strategy. Furthermore, the Electoral Tribunal considered that the proof offered showed that the tweets had been paid through intermediaries. *Unknown* (2016)	Freedom of expression	
10	High Chamber of the Federal Electoral Tribunal		VS Equity of elections	Equity of elections
		Source: https://www.rtvslo.si/news-in-english/supreme-court-on-election-blackouts-every-comment-is-not-		
			Freedom of	

RELEVANT CASE LAW – SOCIAL MEDIA				
#	Country /Authority	Case Summary	Legal conflict	Ruling in favor of…
	Slovenia	propaganda/403791	expression	
1 1	Supreme Court of Slovenia	Saša Pelko was fined for posting an interview with the then-candidate for Maribor mayor, Andrej Fištravec, on Facebook, with the comment “Great interview, you’re invited to read it" during the election silence, which lasts the day prior to the elections and the election day. The Supreme Court determined that the regulation violated the freedom of expression and that citizens should be allowed to publish opinions on social networks, forums, and in the media, as well as to make comments in public, without it being considered propaganda.	VS Equity of elections	Freedom of expression
	USA	*Rideout v. Gardner, 14-cv-489-PB* (2015) In 2014, a legal reform prohibited the sharing of digital images or photographs of marked voter ballots on social media.	Freedom of expression	
1 2	U.S. District Court for the District of New Hampshire	Three citizens who shared their ballots on Facebook challenged the law on First Amendment grounds. The Court ruled that the new law is a content-based restriction on speech that cannot survive the standard of strict scrutiny considering that New Hampshire does not have a problem with voter buying or other voter fraud.	VS Equity of elections	Freedom of expression
	Brazil	*Aécio Neves da Cunha v. Twitter Brasil, 1081839-36.2014.8.26.0100* (2015) Aécio Neves da Cunha, Brazilian senator and former presidential candidate, sued Twitter Brazil, requesting the registration data and electronic records of 55 Twitter users, alleging that they posted	Honor VS	Honor (in those cases linking Neves to drug-related criminal activities).
1 3	São Paulo Court of Justice	defamatory content during the election campaign and thereby interfered with the electoral process. The Court ruled that Twitter Brazil must provide Neves with the registration and identification of 20 users who had linked Neves to drug-related criminal activities, but not to the remaining users who had merely shared news links. Twitter Brazil has appealed this decision.	Freedom of expression, Anonymous speech, Freedom of commerce	Freedom of expression, Anonymous speech, freedom of commerce (in those cases of users who had merely shared news links).