Second version of the "Glossary: Digital Media and Elections"

Deliverable of the Observatory on Social Media

Fifth Plenary Assembly of the Global Network on Electoral Justice (GNEJ)

General coordination: Board of the Observatory on Social Media Editorial

Design and coordination: Technical Secretariat of the GNEJ

Academic Coordinator: Rafael Rubio, Professor of Constitutional Law at the Complutense University of Madrid

Global Network on Electoral Justice
BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM
TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

Index

Introduction

Social networks have transformed **electoral campaigns**. Their irruption into society and, above all, their widespread use have led to changes in the way information is disseminated and in the possibilities for political organization, particularly regarding the use of **segmented advertising** in financing mechanisms or the recruitment and organization of volunteers.

These innovations are not exclusive to the electoral campaign but affect the entire process, from the presentation of candidacies to the proclamation of the elected officials. Information technologies have made it possible to extend the exercise of the right to vote (Brazil), facilitate its exercise by improving information with mechanisms such as **QR codes or the use of chatbots**, improve its transparency and the possibilities of control (Indonesia), increase the efficiency of the system and confidence in it (offering results in a reduced time that shortens moments of uncertainty).

During this electoral period, technological threats become more visible, as it is a particularly intense moment that affects the legitimacy of the entire democratic system and in which the mandatory opening of the system to society may pose certain weaknesses. In the electoral period these threats are aimed at the root of the basis of trust in the democratic system, the process of electing representatives, which is where they obtain their legitimacy.

On the one hand, the threats of technological attacks that seek to alter or collapse the system in a general or selective manner have multiplied. The electoral system, even when it relies on a large group of people, depends on technology in key phases, such as the elaboration and distribution of the census or the transmission of the results and their sharing, a dependence that can be even greater in places where it is necessary to request registration to the census or, obviously, in systems that have incorporated electronic voting. In this field, there have been reports of attacks on the census in specific locations, which sought to exclude certain voters from the process or to delay the exercise of the vote by causing crowds that would selectively discourage the exercise of it, or threats to the counting system (Netherlands). The attack on technological infrastructures can also affect the electoral campaign, with the theft of private information (United States in the 2016 presidential campaign), DDSS attacks on websites or the illegal use of databases to deliver messages to a specific group. The global nature of these threats has led to the emergence of different principles and standards to protect the processes and the rights involved in them.[1]

[1] Venice Commission, Principles, for a fundamental rights-compliant use of digital technologies in electoral processes. Opinion 974/2019

Also in electoral campaigns, the **internet** has become a differentiating element; anyone who participates in an election knows that using technology in an innovative way offers a head start advantage. It is not only about quantitative changes that give an advantage to those who adopt innovations earlier; it also involves changes in key elements of the whole electoral process in terms of its channels, actors, and timing. **Web 2.0** (**characterized by user-generated content**), which allows users to publish posts in audio, video, or text format and disseminate this content thanks to other users, giving it **virality**, has turned the companies that provide the connection (**ISP**) and those that provide the software to make these publications (**internet intermediaries**) into real protagonists of the campaigns.

Such is the prominence of technology in these processes that it has even characterized successive electoral processes, at least in the US American presidential campaigns, which are usually ahead in the introduction of technology. Thus, we have been talking about Meetup elections (2004), social networks (2008), micro-segmentation (2012), or Twitter and Facebook advertising (2016).

During the campaign in recent electoral processes it has been possible to see practices such as: the ability to profile users and adapt communication, paid or organic, to these profiles (a practice popularized by the company Cambridge Analytica in the pro-Brexit campaign in the referendum on the United Kingdom's permanence in the European Union held in 2018); the interference of individuals or groups other than political parties, both from inside and outside the territory in which the elections are held, using the purchase of advertising or through coordinated *astroturfing*[2] actions (a practice denounced and demonstrated in the 2016 and 2020 US presidential elections); the creation of fake profiles (automated or manually managed bots) to create favorable opinion currents (as in the 2018 Irish abortion referendum); or the use of interpersonal communication platforms to massively distribute disinformation messages (in which the use of WhatsApp made in the Brazilian presidential campaign by Jair Bolsonaro in 2018 stands out).[3]

The perception of increased risks to democracy in this period is causing an evolution of legal responses that initially sought to provide a solution to new phenomena by applying flexible interpretation of existing rules with a strong component of case-law creation and a significant dependence on technological operators (Rubio, 2018). Faced with the quantity and intensity of threats, we are currently witnessing a change of trend, a regulatory impulse of proactive limitation of certain practices and tools in the field of disinformation, segmentation, and political advertising, closely related to each other and in which technology plays a special role.

[2] Anónimo. Confesiones de un bot ruso. Debate, 2022.
[3] Óscar Sánchez Muñoz, La regulación de las campañas en la era digital. Desinformación y microsegmentación en las redes sociales con fines electorales, Cepc (2020).

There is a positive obligation to ensure conditions in which the electorate can freely form and express its opinion and choose its representatives (**the right to vote and to be voted for**). Freedom of expression (especially in political debate) and free elections are mutually necessary rights. Thus, it is essential to adapt the legal framework in this new context to ensure the conditions for a fair electoral environment, which in the digital scenario implies a series of added difficulties to protect the freedom and secrecy of the vote to keep freedom of expression safe and not to harm the principle of fairness. To do so, for the time being, we must resort to the general principles that affect campaign periods, such as the electoral ban or the financing of electoral campaigns and their control, which becomes much more complex.

In this line, familiarizing legal operators with the most common concepts in this field, as well as with regulations and jurisdictional decisions on the matter, contributes to improve the response to this growing threat which must necessarily be hybrid and global. This work is based on the *Glossary: Digital Media and Elections* of the Observatory on Social Media of the Global Network on Electoral Justice and, on that basis, the Network develops it by offering a general and integrated vision of cases and concepts which, for clarity and ease of identification, we have highlighted in bold letters.

I. Surveillance: The origin of all our woes?

Rodrigo Cetina Presuel
Law Professor
Universitat Pompeu Fabra Barcelona School of Management
Harvard Law School
6odrigo.cetina@bsm.upf.edu

In recent years it has become evident that political manipulation and attempts to unduly interfere with electoral processes around the world have become commonplace and that social media are at the center of these concerns. It is also evident that social media platforms have a disinformation, misinformation, and malinformation problem. And while the dissemination of falsehoods, inaccurate or damaging information or attempts at manipulating public opinion are nothing new, it has become clear that social media platforms exacerbate problems related to these phenomena by virtue of their characteristics (not at all unique, some are shared with other ICTs and other media): dissemination of information is non-hierarchical, spreads with great speed and often virally among networks of connected users, etc. More singular characteristics (although also present in other internet media) include that messages can also be delivered using microtargeting and personalization techniques to disseminate all kinds of information to targeted, specific, groups of users and which make it very difficult to figure out which groups are being exposed to what messages (see echo chambers, epistemic bubbles), and that the spread of information is somewhat faster than with others and that the production economy of content is different as well.

Glossary

Of all the concepts that ought to be considered we should first refer to *surveillance,* because, as said before, this concept underlies all logics that operate to yield the problems this work explores in relation to election interference.

Surveillance is the collection and processing of personal information for care or control and that enables the identification, tracking and categorization of people or groups of people. While surveillance practices have existed for a long time and the systemizing monitoring of populations and individuals is a distinguishable characteristic of the modern state (an activity known as state surveillance), contemporary surveillance adds two other defining characteristics, namely, that it is digital surveillance, defined as the collection and processing of computerized personal data; and that many internet-based private companies engage in the surveillance of their users for their own private goals and not necessarily by governmental mandate, a set of activities known as private surveillance.

Apart from defining *surveillance*, we must necessarily define related topics since the concept of surveillance is underlying in the logics that operate in most problems related to election interference and political manipulation. This makes it necessary, then, to define different subcategories of surveillance should also be properly defined, alongside other related terms to allow to create a full picture of the concepts and a better understanding of them, together and separate.

These concepts include *state surveillance* or surveillance activities carried out by the state and in pursuit of governmental goals. Systemic monitoring of populations and individuals has become a distinguishable characteristic of the modern state. *Private surveillance* is defined as surveillance activities carried out by private entities that are not part of government. Internet-based private companies engage in the digital surveillance of their users for their own private goals and not necessarily by governmental mandate, even though they may provide surveillance services or supply surveillance technology to governments and their agencies. It also includes *digital surveillance*, or the collection and processing of computerized personal data and that enables the identification, tracking and categorization of people or groups of people as well as online surveillance (social media surveillance), which is any digital surveillance activities carried out online and on social media platforms. For the companies that own social media, this is an essential practice at the center of the monetization of their profit-making activities. For governments, the internet, and particularly social media, have become a space for the surveillance of citizens for various political and electoral goals. It also includes the concepts of *private-public digital surveillance*, which is the imbrication of surveillance activities and goals carried out by the state and by private entities. Often, it implies the reliance on private surveillance technology for state goals that governments would not be able to achieve on their own. Crucially, another key concept is *digital political surveillance*, which is the use of social media platforms to monitor citizens, inhibit their political action and silence dissent.

Then, we have other concepts that help us paint a proper picture of the current state of surveillance online, which are *surveillance capitalism*, defined as form of information capitalism in which the economic system is centered around the collection of personal data to enable the prediction and modification of human behavior to produce revenue and achieve market control.[4] Another one is *instrumentarianism,* which is the instrumentation and instrumentalization of human behavior for the purposes of modification, prediction, monetization, and control. [5] As defined by Zubboff, it is a concept intimately related to surveillance capitalism.

[4] Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5
[5]Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. New Labor Forum, 28(1), 10–29. https://doi.org/10.1177/1095796018819461, p. 20.

Active private surveillance by social media platforms has made them stand out from other types of media. This socio-technical capability of recording and monitoring every action a user undertakes online not only allows social media platforms to build complex (if inaccurate) profiles of their users that in turn allows them to separate them into groups and serve personalized content, but it is also mostly what underlies the business model of social media companies. They seek profit through user surveillance, the extraction and processing of their personal data and either the sale of these data, of user profiles or by enabling systems that allow them to sell personalized advertising (including targeted political advertising) or serve personalized content, whichever is the most likely to keep a user engaged and using the platform, and in turn extract more information about them in order to monetize it some more, and so on.

The digital private surveillance industry has grown and sophisticated itself by developing technology that far exceeds the surveillance capabilities of the state. Governments have started contracting surveillance services from private entities and piggybacking or using technology that originally serves a private surveillance purpose that is then repurposed for state surveillance. Private and public surveillance combine to yield a massive corporate-state surveillance apparatus. A public-private partnership from hell.

Private interests and public interests have made digital surveillance technology ubiquitous. Digital surveillance capabilities have expanded and sophisticated themselves to cover all kinds of people in all kinds of places and situations. As said before, private surveillance itself has grown into its own - very large - part of the digital industry as it allows for profit-making through the selling of data and the selling of advertising. Digital private surveillance of users has become so central to the internet as we know it that some people describe this economic model as a subset of capitalism, calling it surveillance capitalism.

Surveillance, however, is not only at the center of social media platforms' business model, it may also be at the center of many of the woes we associate with social media platforms: invasion of privacy, infringing on a right to personal data protection (which implies control of data about oneself), dissemination of hateful speech, the enabling of online abuse, the spread of targeted content and targeted advertising (sometimes with the intention to manipulate or disinform), and it may also be one of the central causes of the phenomenon of online disinformation itself.

This is because social media platforms do not base their business model on serving content to their users or keeping them connected or on being the best possible means of receiving the news, keeping them well informed, or on enhancing public opinion and political debate. Despite what one may hear, the promotion of free expression or a free press is also not central to their way of doing business. Surveillance of their users is.

Under the logics of surveillance capitalism, social media platforms seek to provide users with any content that may keep them using the platform as increased user-activity leads to increased surveillance of the user, or in other words, increased opportunities to monitor users and extract data that can be turned into profit one way or the other.

This has made social media platforms information-agnostic. This means that platforms' main concern is to disseminate any information to any user if it can keep that user engaged and using the platform even if it could be disinformation, malinformation, or misinformation and regardless of if the content is inflammatory, abusive, or manipulatory. It also means that the creation of echo chambers through targeted distribution of information, messages, or advertising is a secondary concern if it keeps users engaged. In other words, a business model focused on surveillance gives the platforms an incentive to be as information agnostic as possible. Anything goes as long as attention spans are kept on the platforms.

Through the socio-technical tool of surveillance, quality information (but also the bad kind) is seen just as a tool, a means to another end, and not a central concern. Social media platforms are merely a set of tools, a group of digital techniques to disseminate messages, and in the wrong hands, they can be used for more nefarious goals that create electoral turmoil, political instability, and can undermine democratic processes and institutions.

Social media platforms are no longer blind to these problems and it is true that alongside regulators and civil society, they are taking steps to mitigate the negative effects of online disinformation. However, if they let the problem fester and become systemic, if they did not notice it was there until the first accounts of election interfering, of attempts to topple democratic institutions through the spread of false information that led to very real political violence, including gender and ethnic-based violence, this is because addressing these issues was not at the center of how they operate, at least not at first.

While it is true that, after being engaged in scandal after scandal and suffering from the public relations fallout and under significant political and regulatory pressure from governments to act, social media platforms have begun to engage in monitoring more actively, filtering, and moderating the most noxious of content, the fact remains that the net result has been negative for democracies and citizens around the world.

Private and public digital surveillance and private-public digital surveillance carry specific risks for citizens and imperil their rights and well-being. Some of these risks undermine political participation directly and surveillance is the underlying activity behind other practices that also result in negative affectations for democracy, including the spreading of disinformation, political manipulation, and electoral interfering.

According to the European Union, political surveillance on social media can help enable governments to monitor citizens, inhibit their political action and silence dissent. Social media surveillance leads to the loss of privacy and autonomy as it undermines citizen´s capacities for political judgement and can lead to political disengagement as the promotion of viral content and addictive behavior on social media can distract people away from politics.

In turn, personalization fueled by surveillance locks citizens in informational bubbles and affects their capacity to form opinions, narrowing their worldviews. Personalization also leads to social and political fragmentation as the segmentation of information and engagement reduces opportunities for political dialogue.

Personalization fueled by surveillance can also aid disinformation by helping distort views and preferences through the spread of false information online and its dissemination can distort electoral outcomes, undermining the integrity of elections and affecting electoral results. Surveillance is also key in enabling automated disinformation as automated accounts can rely on user-profiles to amplify and exacerbate the effects of false information.

It is particularly important that these concepts are appropriately defined to be able to comprehend them better and to contribute to properly identify those undesirable uses of the techniques and to adopt measures to resist them. This contribution contains the definition of several of the aforementioned concepts as well as other related ones, building up on previous work that has yielded a glossary of terms related to how technology is used for interfering with elections and political manipulation online and has classified them in a way that allow for the building of a map of related terms.
To complement those definitions, we have also conducted an analysis of case law and legislation that deals with those concepts, and in the case of this chapter, specifically with the concept and activity of surveillance. The goal of this is shedding light on what the law and the courts have to say about it, its legal definition and legal limits, including how online surveillance can undermine the fundamental rights of citizens and if the law properly recognizes that surveillance enables political manipulation, election interference, and can be a threat to electoral processes and democratic institutions by extension as well as what responses to its negative effects exist in the law.

Cases

Concretely, this work includes an analysis of several cases reviewed by the Spanish Junta Electoral Central (Central Electoral Board or JEC in Spanish). All those cases are related to electoral campaigns and have direct and indirect relation to the use of surveillance to deliver political messages and electoral propaganda, particularly within the context of the General Elections Regulation (or LOREG in Spanish). Twenty-eight cases and instructions spanning the period from 2011 to 2021 are reviewed along with another related case that dates back to 2006. Some of these cases are requests for

approvals, some are consultations, and some are instructions issued in relation to interpretation of electoral and political campaign rules, some are complaints against political parties, politicians, or government bodies.

One decision from the Spanish Constitutional Court that addresses the constitutionality of some provisions of the general electoral law related to safeguarding fundamental rights, including the right to personal data protection related to political opinions is also reviewed as well as a case before the Mexican Electoral Board that analyzes the nature of social media and the distribution of political opinions and electoral propaganda through them as well as another case from Colombia's National Electoral Council that similarly ponders the nature of social media and its capabilities for both targeting users and deliver political messages and electoral propaganda to the masses.

An assessment of analyzed cases ponders their implications for digital surveillance and what this means for electoral processes and the use of social media in ways that strengthen, not hinder, political debate, informed political choice and strong democratic political processes.

In the case of Spain, based on the cases reviewed, the Electoral Board has interpreted relevant laws related to electoral communications to include all forms of online communications. However, it seems that the JEC has not directly grappled with the implications that surveillance, microtargeting, and the creation of online profiles can have regarding how messages can be delivered online and thus is yet to grapple more directly with requirements such as transparency or the monitoring of online campaign spending in order to guarantee free and fair elections as social media continues to be a central tool in modern electoral communications.

However, the Spanish Constitutional Court did strike down an article of the Spanish Electoral Law (art. 58 bis 1) that would have allowed political parties to gather and process personal data related to the political opinions of citizens for not offering sufficient appropriate safeguards to the rights and data of citizens and by not being able to clearly define what public interest and constitutional interests it sought to pursue. This has strong and direct implications, particularly for political surveillance in Spain. Together with the national data protection law and the European Data Protection Regulation, it serves as a strong framework to protect the data protection rights of citizens and, in this case, provide strong protections for data protection as an instrument for protecting the freedom to hold and express political opinions guaranteed by the Spanish Constitution and the European framework of fundamental rights protection.

In the case of Mexico, it is clear that, at least in the reviewed case, the Mexican Electoral Board did not demonstrate enough sophistication in their understanding of how the modern internet works, and particularly how social media work. The Board's

commitment to setting a high bar to limit freedom of expression as well as the freedom to express preference for one or another political candidate is laudable, including protecting those rights for family members of political candidates. However, besides passing references to the internet being different to other media and including a definition of microtargeting, and even of *influencer,* it fails to acknowledge other important concepts such as organic marketing and the virality of posts and ascribes a "presumption of spontaneity" to all social media posts that is at odds with how social media is used for any goal even tangentially related to commercial, political, or electoral goals. The Mexican electoral authority criterion is that social media and the internet are so different from media such as television or radio that their electoral law should not apply to communications done through online means, which seems old fashioned. If anything, this may signal that Mexican electoral law is overdue for a change to include online electoral communications in order to properly set the rules of the game and keep Mexican electoral law in line with where other countries are going.

Finally, the case of Colombia is interesting for the opposite reasons; it demonstrates a more sophisticated understanding of social media by that country's National Electoral Council, resolving on a case about electoral communications done outside the period that the law allows. While the Council granted that according to criteria followed up until then, the infraction should not be subject to a penalty, it does recognize that such criteria should change given the nature of the internet and signals that it will do so in the future. Interestingly, it takes into account how communications are in fact distributed on the internet, both allowing messages to be directly targeted to specific groups of users, but also understanding that those messages can also be made widely available to indetermined groups of people, and that sometimes that is precisely the strategy of those that intend to distribute electoral communications online.

II. Disinformation

Vitor de Andrade Monteiro

Lies, rumors and deceit have never been external to politics. In fact, dissimulation and falsehood are figures that have always been present in political disputes and in the atmosphere of the democratic environment. Some historians claim that even the context of what has come to be known as the framework of the emergence of democracy in Athens carries some falsehood. It is suggested that the motives for the heroic tyrannicide of Hipparchus by Harmodius and Aristogitus, which led to the establishment of democracy in Athens a few years later had more to do with passionate and selfish reasons than with a noble democratic spirit. In spite of this, the false story has triumphed and the lovers were recognized as the founders of democracy, having received tributes and their descendants obtaining honors and privileges.

In ancient Rome, misinformative dossiers were used by emperors to seek legitimacy and ensure the stability of their government. Septimius Severus, although he had no family ties with his predecessor, Commodus, who was the illegitimate son of Marcus Aurelius, tried to create a false relationship with this famous emperor, so that he would be accepted by the population as the most legitimate successor. Since a considerable part of the Roman population could not read and news was reproduced mainly through images, he ordered the minting of coins with his image duly retouched to present physical features similar to Marcus Aurelius and strengthen his acceptance by the Roman population.

Given this long-standing relationship between lies and politics, it is worth asking why discussions about lies in politics have become so important today. Why are ***fake news*** the subject of so many debates and concerns for electoral bodies? In other words, if falsehood has always existed in politics, why is it still important to discuss **disinformation**?

The search for answers to these questions seems to go through two points. One is the phenomenon of **post-truth**, and its impact on the understanding of lies (and truth!) today; the other is the advent of digital platforms and all the revolution it has brought about in the field of communication that derives from it. Although the scope of this paper does not allow for an in-depth analysis of each of the aforementioned points, the development of the central theme of this paper requires a passage, however brief, through them.

The term **post-truth** is presented as an expression of effect that serves to capture a panorama of current times. It represents the decline of rationality, the obfuscation of facts, the overcoming of comprehensible reality by a logic guided by emotion, belief, and subjectivity. In post-truth times, objective and verifiable facts have less influence on **public opinion** than individual beliefs. Rather, there are no facts, but

interpretations of facts. It is the victory of *doxa* over *episteme*, of opinion over knowledge. A scientific study, methodologically correct and contrasted by the academic community, has the same weight as a legal opinion.

The fluidity of current times does not allow for exhaustive - and tedious - reflections and the conclusions seem to follow this dynamic. It is the triumph of the liver over the brain, of the apparently simple over the honestly complex. In this scenario, the search for truth has been replaced by the construction of a version of the facts that brings satisfaction and offers protection against the harshness of reality. This reclusion in subjectivity directs thought towards a welcoming environment, which offers opinions that reinforce pre-existing convictions, even if they are founded in nothing. It is the perfect environment for the development of **meta-narratives**, **conspiracy theories** and **alternative realities** of various kinds, all of which contribute to the devaluation of truth as an element in political decision-making.

This shift away from the idea of truth is add to the impact of new technologies on the **information ecosystem**. With the vertiginous growth of digital media communication and its deeper insertion in society, there have been significant changes of various kinds. The informality with which communication develops in the digital environment, while democratizing the right to express an opinion has ended up enhancing the effects of post-truth, since it has made possible a relatively balanced competition between scientifically proven facts and professional journalistic texts, on the one hand, and unsubstantiated opinions and the resignification of facts on the other. This is more striking in view of the immense volume of content produced every minute on social networks.

On the other hand, the business model of digital platforms encourages the amplification of misinformation, as it is based on capitalizing on the attention and participation of users. False information spreads much faster, farther and deeper than true information, and therefore generates more profit. The harmful effects of misinformation are observed in various contexts of life in society, from decisions on issues related to economic and public health problems, in the evaluation of drug policies, in religious issues, etc. However, it is the political context that appears to be most susceptible to the influence of **manipulated information**, with false information on this topic having been found to spread significantly faster, farther, deeper and more widely than others relating to terrorism, natural disasters, science and urban legends (VOSOUGHI et al., 2018).

Disinformation undermines the ground on which dialogue is built, encouraging the use of force as a means to resolve different opinions. Democracy loses space since its existence depends on the free and unimpeded circulation of ideas (STENGEL, 2020). **Information disorders** undermine the right to participate in the electoral process in a conscious and informed manner, which translates into a deficit of legitimacy in the outcome of the elections and damage to the normality of the electoral process.

The electoral process more than offering valid results that correspond to reality in order to achieve its main objective, needs to transmit the sensation of validity and legitimacy.

As Caesar's wife, it is not enough for the electoral justice to act well, but it is necessary to transmit to the voter the perception that the electoral process took place within normality and extracted the true will of the electorate. The institutional mission of the electoral justice requires, therefore, the production of trust and it is precisely on this point where the merchants of disinformation have focused.

A worrying trend has been identified whereby the **informative disorder** in the electoral context is aimed at attacking the integrity of the electoral process and the authorities linked to the electoral body competent for its realization. This strategy, constantly associated with some kind of **digital populism** (BRUZZONE, 2021), has been identified in several countries around the world, as exemplified by the last presidential elections in the United States, the Brexit vote, the Brazilian elections of 2018 and 2020, the presidential elections in Mexico, Hungary and Peru.

These pernicious artifices tend to impact the credibility of the institutions involved in the process and discredit the results obtained in the elections. This scenario opens the door to pro-rupture movements (as in the case of **Myanmar**) and popular uprisings followed by violence and death (as in **Kenya** and **Ivory Coast**). Moreover, the very existence of the electoral body may be affected by the effects of disinformation, as the loss of reputation paves the way for legislative reactions (such as the loss of powers by the electoral body) and the intensification of attacks aimed at institutional suffocation (such as the reduction of budgets, functional prerogatives and its personnel). A striking example is the case of the **National Electoral Institute of Mexico**, which, after being the victim of several disinformative news, was proposed to be abolished by the president of the republic, Andrés Manuel López Obrador.

The impacts of disinformation can be made more felt with the use of **strategies of automation of profiles** in social networks, allowing manipulated information to be disseminated by ***bots*** with human appearance to promote certain posts, amplification of publications from low credibility sources and mentions to influential users in those publications. With this behavior, *bots* play an important role in the production of the viral effect of disinformation.

Glossary

An adequate understanding of the phenomenon of disinformation requires familiarity with some concepts that translate important characteristics of information disorders. In principle, the very definition of what is inserted in the concept of disinformation is something that demands close attention. For some authors, such as WARDLE and DERAKHSHAN (2017), disinformation is one of the notions that are included in the idea of informational disorders. For them, it is necessary to distinguish messages that are true from those that are false, and even those that are created with the intention of causing harm, from those that are not. Thus, the informative disorders constitute a set that includes the figures of a) **erroneous information** (***misinformation***), which is the one that is produced without the intention that causes damage, but that has false content; b) **disinformation** (***disinformation***), which is content created deliberately to

cause harm; and c) **misinformation** (***malinformation***), which is information based on reality, but which is used with the intention of causing harm to someone, an organization or a State (WARDLE and DERAKHSHAN, 2017).

Despite the long use of the expression ***fake news*** by the media, its use is not recommended for the definition of the phenomenon of disinformation, since it does not allow a clear delimitation of its object nor a correct understanding of the problem. First of all, it should be noted that the expression *fake news* has been used as a weapon that is directed at opponents for their own condition of enemy, and not against information presented by them. Moreover, as we have seen, sometimes the informative disorders include information that in its origin are not *fakes*, as in the case of misinformation. It is also perceived that the very idea of news is linked to something based on truth, which makes the expression *fake news* an oxymoron.

Another important concept for understanding the phenomenon is about ***Information Operations*** or ***Influence Operations***. These consist of a series of warfare techniques used to obtain information and influence and destabilize the adversary's decision-making process. Human disinformative practices are sometimes promoted in an orderly manner by companies dedicated to create and manage profiles to produce ***posts*** and ***likes*** to stimulate a certain narrative. These companies are known as **content** or **click farms**. The figure of trolls is also particularly present in disinformation and consists of users of digital platforms who deliberately seek to threaten, provoke, intimidate and offend to cause distraction or discord. Their actions may be isolated or in an orderly manner with other actors. Sometimes their actions are promoted by companies dedicated to these purposes and that act in the same way as the click farms, and that is why they are known as ***troll farms***.

In the disinformation activity, there are many ways to create narratives and one of the most sophisticated is ***deep fakes***, which consist of the manipulation of images and videos through artificial intelligence to combine real aspects with other fabricated ones, seeking to create ultra-realistic content in which people say or do things that did not happen, creating confusion in the recipient. Disinformation often benefits from reprehensible practices to obtain more results. ***Phishing*** is one of them and it is based on attacks directed by *hackers* to obtain users' personal data.

Cases

Although misinformation is not something new in society, its impact on electoral processes is now receiving more attention from electoral bodies. This text includes several cases judged by the Spanish Central Electoral Board (JEC, in Spanish), by the Superior Electoral Tribunal of Brazil (TSE, in Portuguese) and Argentina that demonstrate the ways in which electoral jurisdictional bodies are dealing with the phenomenon of disinformation through digital platforms in the electoral process. In the sequence, some of these cases are presented, in addition to documents that deal with the challenges of confronting disinformation.

Disinformation affects the voter's ability to choose his or her candidate based on truthful information and ideas that correspond to reality. Thus, access to correct, transparent and accessible information is a requirement for effective freedom. For the **Argentine National Electoral Chamber** in the **Extraordinary Resolution 66/18**, the more information, impartiality and freedom in the electoral process, the higher the quality of democracy. The Chamber recorded the impacts on the amplification of disinformation of ***trolls*** ("paid commentators using fake profiles") and ***bots*** ("simulated profiles with certain moments of intense online activity, followed by long periods of inactivity"). For the institution, in order to achieve any success in the complex task of countering information manipulation, "time, resources and creativity" are needed, starting with special attention to media education. After developing an analysis of the phenomenon in various electoral contexts, the Chamber went on to adopt a series of measures aimed at regulating the participation of participants in the electoral dispute resolution in elections, such as the disclosure of the results of monitoring of social networks and propaganda and the creation of a registry of social network accounts and official websites of candidates, political groups and top electoral authorities.

In the **Agreement 3010/02**, **the Argentine National Electoral Chamber** reiterated the importance of access to information for the exercise of the right to vote, which it called "informed voting". The relevance of **access to information** for **democratic order** has been highlighted in the **Advisory Opinion OC-5/85** of the Inter-American Court of Human Rights, which stated that freedom of expression is a condition for society to make informed decisions. The conclusion of the Court is that a society is not free if it is not well informed, and, evidently, the quality of information is essential for effective freedom.

An important initiative developed by the National Electoral Chamber of Argentina to preserve the quality of the democratic debate on digital platforms is the **Digital Ethical Commitment**. This document takes into account the growing concern with the manipulation of information on digital networks and in the digital environment and its impact on democracy. The Commitment mentions the referred **Agreement 66/18** to register the convenience of promoting digital education to improve the management of electoral political information in the digital environment. By adhering to the commitment, the entities assume the commitment to promote, "the honesty of the democratic debate in the upcoming national elections, so as to contribute to mitigate the negative effects of the dissemination of false content and other disinformation tactics in social networks and other digital environments". At the same time, the adherent digital platforms declare that "They recognize the complexity and tension that may exist during the electoral process with the dissemination or proliferation of inaccurate information or false news, and agree, within the framework of their possibilities and tools, to collaborate with the competent authorities in this process respecting democratic values and freedom of expression". Several digital platforms will adhere to the commitment, such as Google, Twitter, Facebook, Whatsapp, Kwai and Tik Tok.

Social platforms have special relevance in contemporary communications. In this sense, the **Central Electoral Board of Spain**, when judging the **file 293/1215**, **in the Agreement 146/2021** has recognized the predominance of social networks in today's society, understanding that their use is almost essential for candidates and electoral formations. In view of this, the behavior of social networks before the parties cannot be considered a political irrelevance. In fact, the performance of the platforms must observe the principle of equality, not being able to serve as a tool to unbalance the political game. In the face of this finding, it is noted that obligations may arise that go beyond those contained in their contracts of use. Thus, for the Board, the sanction applied by Twitter, of suspension of functions of the profile of an electoral party, due to the breach of its terms of use was reasonable phase to the behavior of the association.

In Brazil, despite the frightening extent that disinformation has reached in the political scenario, there are few cases in which the issue has been debated in the highest electoral court. In two important cases, the TSE has debated the possibility of applying the sanction of loss of mandate due to the **dissemination of disinformation** by candidates and the **use of mass sending** through the Whatsapp application.

The **Franceschini case** deals with the **dissemination of disinformation against the electoral process through social networks** on election day. In short, a deputy made a live broadcast on election day, and before its closing, claiming that they had fraudulent ballot boxes and that he had official information about the fraud. The TSE considered that there were sufficient grounds for dismissal, considering that there had been abuse of media power. According to the data expressed in the ruling, the live broadcast was transmitted live, before the end of the voting (on 07/10/2018), to more than 70,000 people (on 12/11/2018, it had more than 105,000 comments, 400,000 shares and six million views). Among the speeches made on the occasion it has been said that the "ballot boxes are adulterated" and that there were documents from the electoral justice recognizing this claim. The Brazilian Federal Supreme Court (STF), when questioned, confirmed the constitutionality of the TSE's decision.

The issue of the **use of mass sendings** through the Whatsapp application was the subject of the **Bolsonaro/Mourão case**. In court the presidential candidacy was acquitted for lack of solid evidence of the accusation of abuse of economic power and misuse of the media. Although no sanction was imposed in the specific case, the case deserves importance as the ruling established the following thesis: "the use of digital instant messaging applications to promote mass communications containing disinformation and falsehoods to the detriment of adversaries and to the benefit of a candidate may constitute abuse of economic power and misuse of the media, in accordance with **article 22 of LC 64/1990 (the Ineligibility Law)**, depending on the actual seriousness of the conduct, which will be examined in each case".

The phenomenon of disinformation brings new contours to the dimension of the right to freedom of expression. Although the right to **freedom of expression** occupies a central position in the democratic environment, the very existence of a democracy

requires the protection of other constitutional rights that can be undermined by the arbitrary exercise of freedom of expression, especially through the use of information disruption. In the **Joint Action Plan Against Disinformation, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy** state that the right to free, fair and informed participation in political processes is increasingly challenged by the deliberate dissemination on a large scale, and the systematic dissemination of disinformation and demand political determination and coordinated responses. The **American Convention on Human Rights, in its Article 13**, provides for the right to freedom of expression and thought. The issue has been addressed by the IACHR Court in the cases **Olmedo Bustos et al. (2001), Alvarez Ramos vs Venezuela (2019), Urrutia Laubraeaux vs Chile (2020)**. For the IACHR Court there is a double dimension that must be considered in freedom of expression: the social and the individual.

Expressing concern and attention to the phenomenon of disinformation and its implementation with the purpose of **confusing and affecting the rights to make decisions** based on truthful information, which are rights impacted by freedom of expression, the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Representative on Freedom of the Media of the Organization for Security and Cooperation in Europe (OSCE), the OAS Special Rapporteur on Freedom of Expression and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights (ACHPR), have published the following statement: "The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Representative on Freedom of the Media of the Organization for Security and Cooperation in Europe (OSCE), the OAS Special Rapporteur on Freedom of Expression and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights (ACHPR), have issued a **Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda** which seeks to present the characteristics and standards on disinformation, highlighting the need to ensure an enabling environment for freedom of expression.

The **Venice Commission**, in the report "**The impact of information disorder (disinformation) on elections**", highlighted that the Internet has changed the way voters receive political messages and that this change can make it possible for false information to be disseminated on an unprecedented scale.

The cases and studies presented above are just a few examples of how electoral courts have faced the challenges of disinformation in electoral campaigns and the difficulties in confronting it.

III. Micro-Segmentation and Personalization: From Electoral Interference to Political Manipulation

Leyre Burguera Ameave
Professor of Constitutional Law
Law Faculty
National University of Distance Education (UNED, in Spanish)
lburguera@der.uned.es

Any successful electoral campaign requires precise knowledge of who the final recipients of the political message are. The analysis of the interests and concerns of the voters provides clarity to configure an effective electoral communication. This purpose has always been present in the organization of electoral campaigns (through surveys, focus groups, etc.) but it is perhaps now, with the emergence of big data, when we are more aware of its potential and the risks it entails.

Glossary

There are different strategies currently used to influence political messages through disinformation or manipulation with the aim of advancing certain political objectives, including the undermining of the normal development of democratic electoral processes. Among them, the use of **microtargeting** and message personalization techniques to design and elaborate electoral communication deserves special attention.

Political manipulation and attempts to unduly interfere in electoral processes through these two techniques have been taking place all over the world for more than a decade. Paradigmatic cases, such as the Obama campaign of 2012 or the Indian parliamentary elections of 2014, are just two initial examples that later found in the UK (Brexit referendum), France (2017 elections) or the US (Donald Trump or Hillary Clinton campaigns in 2016) a greater impact.

This situation is due, in part, to the expansion of the use of social media and to the fact that the work of collecting and analyzing the data stored in these tools has become more professional and sophisticated over time. As a result, social media have been at the center of concerns about electoral advertising aimed at specific groups of users and the lack of transparency of the process.

The **micro-segmentation** and personalization of the electoral message obey a communicative inertia that does not have to be conceived as negative, since it could favor political motivation and involvement, increasing voter participation in electoral processes.

However, their design and use by political parties does not usually obey this candid intentionality; on the contrary, they try to improve fundraising (in countries where campaign financing is mainly private) and mobilize the electorate to such an extent that they can even encourage negative campaigns, polarizing and fragmenting the electorate itself. They also facilitate interference and the undermining of privacy and the right to personal data protection, as well as the creation of so-called echo chambers and epistemic bubbles.

In addressing the potential risks of these two tools in the text, reference will be made, specifically, to the use of big data and artificial intelligence in this field.

The collection and processing of data by political organizations for political communication purposes together with the use of the aforementioned modern techniques have generated a wide debate and concern regarding the limits to be applied, among which is the right to the protection of personal data.

The problems and challenges that will arise are mainly related to two interconnected issues: obtaining the data necessary for the design of today's "data-driven campaigns" in relation to the respect of personal data protection regulations and determining the uses of such data in connection with the increasingly frequent organized disinformation strategies. To all this, we should add: the vulnerabilities of technological structures and their business models, the variety of devices enabling data collection, the development of artificial intelligence, the regulatory subjection of technology companies, etc.

However, in the specific case of **micro-segmentation,** the risks associated with its use that will be discussed are political manipulation, since this technique reduces the critical capacity of citizens, and distortion of the electoral process, since it can explicitly change the rules and norms.

In the case of **personalization**, the risks associated with its use have to do with the configuration of a limited vision of the world, since it individualizes the information received by citizens, reducing their worldview and feeding it back into a sort of information bubble. In this way, the citizen's capacity to form opinions and be able to understand or comprehend those who think differently is clearly constrained. As a result, it produces social and political fragmentation, reducing the capacity for dialogue of the society in which this technique is inserted.

In short, concerns that have increased with the publication of certain cases of unlawful processing of personal data to influence the political opinion of voters (a paradigmatic case is that of Cambridge Analytica), and which has led to certain countries regulating the issues mentioned here, in a more or less restrictive manner.

This is the case, for example, of the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*) which, on March 6, 2014, issued its document "*Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale*". In November 2016 the French Authority (*Commission Nationale de l'Informatique et des Libertés*) did so with, among others, the title "*Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?*" And in April 2017, the British Authority (Information Commissioner's Office) approved its "Guidance on political campaigning". Likewise, the European Data Protection Supervisor issued on March 18, 2018 its Opinion 3/2018 on "online manipulation and personal data ("EDPS Opinion on online manipulation and personal data") and the European Commission, in view of the approaching 2019 European Parliament elections, on September 12, 2018 approved its guidance on the application of European data protection law in the electoral context ("Commission guidance on the application of Union data protection law in the electoral context").

Likewise, this text is going to include mentions to the two main concepts mentioned above: microtargeting and personalization of politics. It will also point out the importance of examining other concepts related, directly or indirectly, to the two issues raised in this contribution. Hence, in this paper, we will deal with notions or ideas such as Web 2.0, social network, profiling, neuromarketing, epistemic bubble, echo chamber, *big data, deep fake, deep learning, datamining, bots*, etc.

Of all the concepts to be considered, we must first refer to microtargeting, also called "audience targeting", "**microtargeting**" or "micro-segmentation", which is defined as the marketing technique of targeting messages tailored to the personal characteristics of the recipients in order to influence their consumer behavior. It involves targeting messages tailored to the data collected on each individual, combined with data collected at other levels, in order to influence their political positioning and voting behavior.

On the other hand, the **personalization of communication** is the use made of this data collection strategy, which favors an imbalance of power between citizens and the groups that control these data, since it opens the door to information manipulation and political polarization.

Cases

To complement the meaning and application of the terms addressed, an analysis of current regulations and case law of particular relevance will be made.

At the legislative level, significant steps have been taken such as Law No. 19.884 of 2017 enacted in Chile, which regulates, in its art. 2, paid electoral propaganda or the Electoral Act of 1993, enacted in New Zealand, section 3ª, which deems that personal

political opinions are not electoral advertising. We are also going to analyze two electoral codes, both from 2014, which regulate these terms (micro-segmentation and personalization) but from different problematic points of view. In the case of the electoral code of Georgia, its article 51.11 affects these issues by affecting the requirements of public opinion polls. For its part, the electoral code of Japan, in article 235.5, deals with the use of a false name, punishing possible infractions with a fine or imprisonment.

At the case-law level, it is worth highlighting, among others, ruling 76/2019 of May 22, 2019, of the Spanish Constitutional Court that resolves the appeal of unconstitutionality filed by the Ombudsman regarding the first paragraph of article 58 bis of the Organic Law 5/1985 of June 19, 1985, on the general electoral regime, incorporated by Organic Law 3/2018 of December 5, 2018, on the protection of personal data and guarantee of digital rights. In that article 58 bis, it was stated that: "1. The collection of personal data relating to the political opinions of individuals carried out by political parties in the framework of their electoral activities shall be protected in the public interest only when adequate guarantees are provided". The indeterminacy of the expression "adequate guarantees" was decisive for this court to consider the nullity of the legal precept that made possible the collection by political parties of personal data relating to the political opinions of citizens. Previously, the Spanish Data Protection Agency (AEPD, in Spanish), had issued Circular 1/2019, of March 7, in which it interpreted the new article, set some criteria and tried to establish some guarantees. It was not sufficient for the scope of the controversy raised regarding the possibility of elaborating ideological profiles in the service of the personalization of the electoral message.

Likewise, it will also be relevant to examine, among others, the ruling of September 3, 2021, of the Electoral Tribunal of the Judicial Power of the Federation (TEPJF, in Spanish) of Mexico, which studies a case of negative campaign, coming to affirm that "although the political debate has a reinforced protection, confusion should not be generated in the electorate or the citizenship with the political-electoral propaganda, since this has a negative impact on the formation of a conscious and informed opinion for the exercise of the right to vote, which could generate a vicious effect with respect to the configuration of the national political system itself". Therefore, the impact of disinformation carried out through specific techniques of obtaining information and manipulation will be the background that makes us perceive the magnitude of the problem.

Also in the Spanish case, the doctrine of the Central Electoral Board (JEC, in Spanish) is reviewed, from the order given in 2007 that comes to equate the traditional communication instruments or mechanisms with the new tools, without taking into account their potential. Hence, anchored in a regulation with a certainly analogical perspective, it is not able to deal effectively and immediately with many of the challenges that arise in each election. Along this path, we will analyze, as an example,

Instruction 1/2021, of the Central Electoral Board, of May 13, on the dissemination of electoral propaganda by means of mailings in which the addressee is not identified by name (BOE no. 119, of May 19, 2021), which comes to interpret article 39. 3 of the Organic Law of the General Electoral Regime (LOREG, in Spanish), modified by the Third Final Provision of Organic Law 3/2018, of December 5, 2018, on Personal Data Protection and guarantee of digital rights, which introduces the right of voters to oppose their inclusion in the copies of the electoral roll provided to the representatives of the candidacies to send electoral propaganda mailings.

In general, and in relation to the terms analyzed, there are significant cases in which the complaints filed before the JEC are dismissed on the understanding that participation in social networks does not incur in any prohibition (provided that it does not involve any type of commercial contracting for its realization). The boundary between advertising (concealed or not) and information is blurred, especially when mention is made of the internet. The agreements covering the period 2005-2022 are reviewed and studied.

IV. The intervention of third parties in the campaign

Rafael Rubio Núñez
Complutense University, Madrid
Rafa.rubio@der.ucm.es

The generalization of information and communication technologies (**ICTs**) has transformed the nature of **electoral campaigns**, which have gone from being a communicative proposal concentrated in time, led by the candidates and the media, to become a communicative proposal in which third parties have the capacity to directly and effectively influence the final result. This type of influences are not new, and already existed through donations and the participation of public actors in the campaign, but now new subjects are added, especially individuals without a political party or candidate affiliation.

Hence, as a consequence of the generalization of the use of technology in elections, there is an increase in the participation of third parties in the campaign and its impact. Although, initially, this is not a strictly technological problem, with technology it acquires a new dimension. Traditionally, the participation of actors outside the electoral process in electoral campaigns was linked almost exclusively to the financing of electoral campaigns by third parties, either by contributing to the official campaign or by organizing campaigns on specific issues, with the aim of influencing the agenda of the candidates. To these forms of participation by individuals and civil society groups we should also add the intervention of government officials (who should remain neutral in the process) or the media (whose role has been increasingly regulated), which, although they have long been subject to regulation, see their role modified as a result of technology.

The emergence of these new actors, or the transformation of the role of some of the traditional actors without a direct link to candidacies, raises new questions for the existing regulation. It is necessary to offer a legal response to new situations such as the actions of individuals or social organizations that impact the election, the possibility of anonymity, the role of foreign actors in electoral processes, the use of bots, etc., that can threaten the fairness of the electoral contest.

If, as Sartori (1993:76-77) argued, "(t)he autonomy of public opinion (...) enters into crisis, at least into a crisis of vulnerability, with the appearance of radio, and even more so with television", with the new information technologies, the concept of public opinion is radically transformed, converted into a puzzle of group opinions, with no apparent relationship between them, which makes impossible the dialogue that is the essence of the very idea of the shaping of public opinion.

Glossary and cases

Traditionally, the participation in campaigns of the media, candidates, political parties, and authorities has been considered. All other political actors were considered to be outside, or irrelevant in their actions. The irruption of communication technologies altered the playing field and the adaptation of these actors gave them a different role.

In the first place, the use that authorities and public agencies are making of these platforms during the campaign stands out for its abundance. By increasing the frequency of their communication and the forms of dissemination of their actions, they can unbalance the electoral contest with greater frequency and incidence, directly and at the moment of greatest impact, both through publications and the contracting of advertising, affecting the fairness of the process, with the risk of misappropriation of public funds. On this point, perhaps the most common but also the least novel, as it is prior to the internet, is the opinion of electoral bodies such as the JEC or the TEPJF. On the one hand, it is interesting to see how in Mexico the TEPJF (SUP-RAP-288/2009, SUP-RAP-318/2012) has extended to leaders, affiliates, militants, and sympathizers of political parties the constitutional obligations regarding political and electoral propaganda in matters such as the obligation to refrain in the political and electoral debate from denigrating institutions and parties as well as slandering people. "Any reading in the sense that this obligation only constrains political parties is unacceptable". On the other hand, more numerous is the prohibition of achievement campaigns in public acts disseminated by the web or electoral publications in the accounts and official pages of municipalities, ministries, or the presidency (JEC among others: **196/2011; 206/2011; 459/2015; 459/2015; 601/2015; 166/2016; 212/2016; 212/2016; 293/841; 293/842; 293/863; 293/864; 293/869; 293/880; 293/882; 293/891; 293/892; 293/898; 293//901**). This is also a common phenomenon in Mexico, where from the beginning the obligation of neutrality of the authorities is raised, also in social media (**SUP-RAP-57/2010; SUP-RAP 105/2014**), and where the performance of President López Obrador has been the object of special attention by the TEPJF **SUP-REP-139/2019 and accumulated; SUP-REP-142/2019; SUP-REP-185/2020; SUP-REP-193/2021; SUP-REP-312/2021 and accumulated; SUP-REP-382/2021 and accumulated**).

Something similar happens with the media, whose definition is blurring, until it loses its monopoly of electoral information. As Cotino (2008) anticipated 15 years ago, "(t)he traditional mass media are either no longer a basic pillar of the democratic system or, at the very least, they are no longer the only basic pillar. The democratic edifice is supported by many other 'pillars' in the network". The extension to these of the protection and obligations enjoyed by the media is being reconsidered with the emergence of express "media", or "pseudo-media", which take advantage of the facilities of the internet to create ad hoc websites and give them the appearance of a media outlet. These informative platforms, which appear and disappear according to the electoral calendar, are supported by a space on the web, with the sole intention of

dressing themselves with the appearance of reliability enjoyed by the media to reinforce the credibility of certain information, usually distributed through social media with the participation of coordinated networks of activists and bots, which allows them to distribute distorted political information with the "guarantee" of being considered media. Many of these "pseudo-media" that hardly meet the usual standards of rigor, necessary for the exercise of the journalistic profession, become the most distributed sources of information during the campaign, as happened with the 2016 US presidential campaign, with media created and managed from a small town in Macedonia, Veles (Peirano, 2019) or the French presidential elections of 2017, where media such as Sputnik or Russia Today, after creating a French version for the elections, slipped among the most consulted during the whole process, with more than 2 million interactions in one month. A particular phenomenon, usually related to the media, is the publication of information not allowed in certain periods such as the results before the closing of the polls or the polls, days or even weeks before the election. This was the case in **Costa Rica (ST. Supreme Court, 2018)**, where in order to disseminate poll results one must have authorization.

Along with the transformation of the role of traditional actors, the application of technology to electoral campaigns allows, as we have seen, the emergence of new actors that can influence the campaign and increase its impact. As Clift pointed out in 2007, "some individuals and informal groups can use the internet to influence electoral results, independently of the parties". As we have seen, today, disseminating information in favor or against a political option, without any link to official campaigns, with higher audience rates and impact is within the reach of many. Anyone can post a message of support or criticism on their social networks, re-disseminate official campaign messages or even ask their followers to vote. But today these activities can influence election results. This increases the decentralization of electoral campaigns, which increasingly resemble an exchange where many senders communicate with many receivers on different social platforms.

Hence, along with candidates, political parties, and the media, the "usual suspects" of the current electoral regulation, it is necessary to pay attention to the role of organizations and individuals without a formal link to the candidacies and the role of the platforms on which these individuals disseminate campaign-related information. These new actors can be real, such as influencers who, voluntarily or for profit, have started to use their networks to support certain political candidacies, or artificially created by state organizations such as the Russian Internet Research Agency (IRA, in English), which, during the 2016 US presidential campaign, created dozens of groups to promote the instability of the process. A sample of 6 of them made by Jonathan Albrighth (Tow Center for Digital Journalism) points to the generation of more than 340 million interactions during the process (Peirano, 2019).

The **right to vote (to vote and to be voted for)** is directly related to the electoral campaign which, in legal terms, develops in a continuous balance between **freedom**

of expression and association, a right that is reinforced in the political sphere and especially in the electoral campaign, and the fairness of the campaign. As stated by the Inter-American Court of Human Rights (2004, paragraph 88), "(t)he exercise of political rights and freedom of thought and expression are intimately linked and mutually reinforcing", but we cannot ignore that this participation of third parties, protected in the exercise of their fundamental rights, can affect the **fairness** of the contest, which aims to ensure that candidates have equal opportunities, and therefore affects other fundamental rights such as the right to vote. Inequity is closely related to the **freedom of suffrage**, assuming that a greater exposure of a candidacy conditions the free participation of the voter, and with the authenticity of the same, avoiding interferences that distort the will of the citizenry; in this case, providing certainty on the origin, destination and limit of the resources used in political campaigns, to prevent political options from obtaining undue advantages.

The **right to vote** requires active intervention to ensure the conditions in which the electorate can freely form and express its opinion and elect its representatives. Freedom of expression (especially in political debate) and free elections are mutually necessary rights, but there is no doubt that, on occasions, electoral fairness may conflict with the freedom of expression of third parties. Thus, it is essential to adapt the legal framework to the legal obligations regarding freedom of expression with the new dynamics of electoral campaigning. In this new context, guaranteeing the conditions for an equitable campaign environment in the digital scenario implies a series of added difficulties, which make it possible to keep freedom of expression safe without harming the principle of equity.

Thus, the general rule has been to consider these activities of individuals during the electoral campaign as an exercise of **freedom of expression**, understanding this behavior as a spontaneous, free, and individual conduct, protected by the difficulty that these individuals have to influence in a decisive way and, in the case that this capacity exists, the legitimacy of their public action. The problem arises in cases in which doubts can be raised about the spontaneity of these actions, with **interference** both internally and by **foreign actors**. These activities can be clearly detected when there is a payment for these interventions and with more doubts when there are forms of coordinated action that could imply a relationship with the campaign, affecting the **cleanliness and fairness of the election**.

The generalization of **web 2.0**, with the **extension of user-generated content** (blog **posts**, videos, photos...), facilitates the participation of individuals with the capacity to influence (**influencer**). In Time, Inc. v. Firestone, 424 U.S. 448 (1976), the Supreme Court defined public figures as those who enjoy special relevance in the perception of society, have the capacity to exert influence and persuasion in the discussion of matters of public interest, and develop an active participation in the discussion of specific public controversies with the purpose of tipping the balance in the resolution of the issues involved. This capacity of influence thus threatens the general rule,

especially when the number of people who are assumed to have the capacity to influence through social media is generalized and extended, or perform these conducts outside of them, amplifying their effects through these channels (**SUP-REC-1874/2021 and SUP-REC-1876/2021 and accumulated**), especially when they do so in a paid and coordinated manner through **influence campaigns**. In this line, different electoral bodies have voiced their opinion, especially the INE and the TEPJF, regarding the prohibition of this type of support campaigns during the electoral silence. They refer to the campaigns in support of the Green Party during the electoral silence of the 2015 and 2021 elections, as well as to the obligation to report the expenses made in this matter for transparency purposes and to calculate the electoral ceiling (**SUP-REP-542/2015 and accumulated and SUP-RAP-172/2021**), as these were coordinated actions in which the payment to some of the participants was demonstrated.

Also, **the ST. Regional Electoral Tribunal, Rio de Janeiro**, **2018** forced the withdrawal of posts published by **bloggers** indicating their desire for the nomination of a particular candidate before the start of the election campaign. It is worth noting that three other rulings of **the TEPJF (SUP-REC-00887-2018 and SUP-RAP-180/2021 and accumulated and SUP-REC 143/2021)** allow this type of third parties to make specific endorsements, as long as they do not receive any type of remuneration, thereby establishing a sort of presumption of spontaneity.

In this context, inauthentic behaviors also emerge as a form of electoral influence of new actors. These are largely based on **anonymity**, facilitated by technology. From anonymity, the third parties we are studying could carry out campaigns that would take advantage of the freedom of not being subject to electoral regulation to bend the rules of the electoral campaign in terms of content, with negative campaigns, or by publishing information that is not allowed during the closed season, thus avoiding the control that we have already mentioned on actions carried out by people with proven capacity of influence. Anonymity makes identification difficult, even impossible; it opens the door to **identity theft** and implies additional complexity for the control and imputation of responsibilities in the event of infringement of the established prohibitions.

Thus, it is necessary to identify the subjects that carry out activities with electoral repercussions, such as the creation of informative pages that disseminate false information about candidates or contract political advertising during the campaign. It is necessary to be transparent about the person or group that is financing them and the way they do it. We find some examples of this type of campaigns, and the response offered by the electoral bodies, in the decision of the **JEC of Spain (688/2019)** on the campaign allegedly promoted by people pretending to be supporters to discourage voting for rival candidacies, or the **ruling of the Tribunal of Sao Paulo (2015)** by which Twitter had to provide the candidate with data of the users who defamed him in said social network. This is in the same line as the judgment of the **Supreme Court**

of Illinois (2015) and, in a documented and systematic way, the **Report on the Investigation into Russian Interference in the 2016 Presidential Election of the United States Department of Justice. However, in other cases, such as the "*Voto útil*"** platform, which provided tools to identify the political option with the highest probability of defeating Morena's candidates in the federal elections of June 6, 2021, by offering public information and there not being any type of linkage, it was considered to be adjusted to the electoral regulations **(SUP-REP-319/2021)**.

Closely related to anonymity is the massive use of **bots**, "fake" accounts, anonymous and automated, which are presented on the networks as another user with the aim of increasing the volume of distribution of certain information, seeking to make it appear to be the majority, artificially creating a current of opinion, of acceptance or rejection of certain ideas or people (Sánchez Muñoz 2020: 34-40). Although platforms are aware of them and act habitually to eliminate them from the public arena, the ease of creating and managing them through artificial intelligence mechanisms has created a real technological war to which the states attend as mere spectators, while the decisions of the platforms, usually without a clear or guaranteeing procedure, can jeopardize the fundamental rights of individuals involved, who see how their accounts are eliminated, without being able to do anything to avoid it or recover them. A related type of threat is that of **trolls**, who, from their personal accounts, use anonymity or false accounts to contaminate the conversation, sometimes even threatening with physical violence, often through coordinated campaigns of inauthentic behavior.

The purchase of **political advertising (electioneering)** in social media can also raise problems related to its contracting by third parties. There are countries, such as **Albania,** that prohibit the contracting of election advertising to those subjects that do not participate in the elections **(Electoral Code of 2012, art. 84),** or **Canada,** that distinguishes advertising from personal opinion expressed in networks **(Electoral Law, section 319)**. However, this prohibition is not universal, and there is always, in addition, the possibility of contracting advertising in electoral time with electoral intent, even if it is not identified as such. While in campaigns supporting a candidate there is no doubt about the need to count a contribution in kind as such, when it comes to campaigns attacking other candidates, the problem becomes more complicated. Take, for instance, Colombia during the last presidential campaign or thematic advertising that is not directly identified with any candidate. In these cases, new conflicts arise related to the coordination, or lack thereof, of these actions with the official campaign, or with the submission of these advertising campaigns to the electoral deadlines that restrict advertising to official campaign time and prohibit it in closed or electoral reflection periods. This purchase affects third parties outside the campaign (**Report on the Investigation into Russian Interference in the 2016 Presidential Election of the United States Department of Justice, JEC of Spain (688/2019) or Recurso em Representação nº 060147858 and the Agravo Regimental em Recurso Especial Eleitoral nº 060505606** resolved by the **Superior Electoral Tribunal of Brazil)**. There is also the purchase of advertising from media or pseudo-media, which

pretend to advertise their content to try to influence the campaign **(Costa Rica, XX)**, as well as the purchase by governmental entities, which in this way improperly intervene in the campaign.

The actions of third parties during the campaign also affect the decisions of the platforms, when in coordination with the electoral bodies or on their own initiative, they adopt decisions that restrict this freedom of expression, such as the closure or suspension of accounts, or the removal of certain content, without a previously known procedure, which opens the door to abuse and arbitrariness, especially when these decisions are adopted in an automated manner by opaque algorithms. These actions, which are often witnessed by states as spectators, are taken without the necessary guarantees to protect the rights affected, as if the fact that they are private companies exempted them from respecting fundamental rights. To guarantee them, these decisions should be adopted, at least during the electoral period, by the electoral bodies or at least through a clear, transparent, and non-discriminatory procedure in which there is the possibility of appealing the decision, and even the obligation to give a reasoned response to it, subject to the subsequent control of a judicial authority. Currently, there is the paradox that since these closures are private individuals they are not considered electoral matters, and do not enjoy the protection of electoral bodies whose action is limited to cases of accounts related to parties and candidates such as the closure of the official Twitter account of the political party Vox during the Catalan elections (2021) or the elimination of WhatsApp channels of all political parties in the general elections of April 2019. In the case of contracting third-party advertising, in the absence of clear regulation, platforms initially opted to label advertising of this nature as political and provide information on the people who have paid for such advertising (so that electoral bodies can consider these payments as campaign contributions and include them in the reports and apply them to the spending ceiling). In some countries, platforms themselves have ended up prohibiting the contracting of electoral advertising to any actor that is not officially part of the campaign (parties and candidates, of whom they require special identification).

In addition, it is important to point out that all the aforementioned conducts can be carried out from inside or outside the space where the elections are held. This refers to the actions of individuals, groups, or even the media, located "virtually" outside our borders, which from their "extraterritoriality" can carry out impermissible actions aimed at influencing the electoral process **(interference campaigns)**. This phenomenon, which first became evident for the first time in the 2016 US presidential campaign, with the proven Russian interference, has been increasing since then (Oxford 16 onwards), and poses challenges to the existing regulation with the purchase of advertising on digital platforms during the day of reflection (electoral closure), or the publication of electoral information, such as the result of exit polls, during the same election day, something usually prohibited. These campaigns also take advantage of their anonymity to promote **astroturfing** actions from fake profiles, which are much more difficult to control. Although the platforms have begun to take measures to avoid these

external interferences, this type of intervention poses new problems of control, proof, and adoption of measures, and the prohibition of any type of action with electoral content from abroad (identified or anonymous, legal, or illegal) is increasingly being considered, for which the collaboration of the platforms is essential.

Conclusions

All the above raises a debate on the role of citizens and groups in the electoral campaign and the establishment of obligations and limits to their activities, in terms of vote solicitation (unofficial campaigns), criticism of parties or candidates (negative campaigns), sending unsolicited information to their contacts or hiring advertising in support or to the detriment of a particular option. Beyond the legitimate exercise of freedom of expression, these new possibilities of participation in the campaign open the door to new strategies of parties and candidates, who can rely on third parties to carry out actions which, due to their content, the moment they are carried out, or their cost, cannot be executed in their own name. In addition, another possibility opens for independent groups without any connection to parties and candidates to influence the results in legitimate exercise of their freedom of expression, in defense of their ideas and/or interests. This is something that, if carried out on a large scale, can affect the fairness of the campaign and create a shadow zone in the existing electoral regulation.

To date, the response has been focused on financial control, which is indispensable to guarantee fairness. During the electoral period, in order to guarantee equal opportunities among political forces, limits are established on campaign expenses, and greater transparency of this financing is demanded by obliging the actors involved to provide information on campaign expenses during the elections, improving the effectiveness of the supervision of the control of electoral campaigns and establishing sanctions for non-compliance in this matter, which can range from the exclusion of a candidacy or the annulment of the election to the total or partial loss of public financing. Including within this control the actions of third parties that have been the object of payment or that are considered to have been carried out for a future expectation is a matter of leveling the playing field, not without difficulties, as we shall see below.

It is therefore necessary to clearly define the response of the electoral authorities to the actions of third parties in electoral processes at a time when they can be decisive, providing an appropriate legal framework.

V. Hate speech and gender-based political violence

Ignacio Álvarez Rodríguez
Associate Professor of Constitutional Law
Faculty of Law
Complutense University of Madrid
ialvarez1@ucm.es

It is important to reach a minimum academic consensus on the object of study, as experts point out that it is too broad. We rely on three institutions that have produced enlightening working papers on the subject. One is the *National Democratic Institute*. Another is the *Observatory of Political Reforms in Latin America* (1978-2021), attached to the Institute for Legal Research (IIJ-UNAM) and the Organization of American States. The third is the *National Electoral Institute* of Mexico.

Glossary

In order to explore the legal framework for so-called gender-based political violence (VPG, in Spanish) during the election campaign, it is necessary to use a series of technical terms, which are included in the Glossary.

The first term is *ciberdelincuencia*, also sometimes called **cybercrime**, a notion that includes all criminal or illegal activity carried out over the internet. Examples include *phishing*, misuse of personal information, various forms of hacking, hate speech and incitement to terrorism, and even the distribution of child pornography and sexual practices involving minors. These types of crimes take place with respect to all digital devices, including computers, tablets and smartphones that are connected to the internet.

Secondly, we must highlight **gender disinformation**, that is, the use of false information to confuse or mislead by manipulating gender as a fundamental social divide to attack women and/or influence political outcomes.

Thirdly, it highlights the concept of **hate speech**, which covers many forms of expressions or attacks that disseminate, incite, promote or justify hatred, violence and discrimination against a person or group of people for the most varied reasons. It also covers polarizing discourse that promotes intolerance, hatred and incitement to violence through explicit or indirect references to race, national or ethnic origin, religion, gender, sexual orientation, age or disability or other immutable groupings, generally with the aim of generating a tangible difference in an institution, organization or society.

Fourth, we have the so-called Internet ***trolls***. Trolls are human users who intentionally harass, provoke, or bully others, often to distract and sow confusion or discord. Trolls may act as individuals and, in this sense, share many characteristics of those who engage in hate speech in analog formats. They may also act through coordinated behavior with other trolls.

Fifth, we should highlight ***online violence against women in politics***, defined as all forms of aggression, coercion, and intimidation of women in cyberspace simply because they are women. It is also known as cyber-violence against women. The phenomenon is exacerbated when done on the Internet because politically active women candidates face various threats from other candidates, parties, and/or citizens.

International and national regulations

There is some international support for the prosecution of violent conduct against women in politics, both from Universal International Law (United Nations) and Regional International Law (European Union, Council of Europe, Organization of American States).

The same can be said of a number of individual countries, although support is scarcer and, when it is forthcoming, rather vague and imprecise. Some have specific legislation on the subject or have attempted to adopt such initiatives (Chile, Argentina, Germany, Bolivia, Bosnia and Herzegovina, Brazil, Ecuador, El Salvador, Mexico, Panama, Paraguay) and others have non-specific legislation that is applicable to such cases thanks to the criminalization of hate speech (Spain).

Constitutional examples:

1. Proposed Constitutional Text for Chile, 2022 (rejected in referendum in September of the same year), Article 27: "1. All women, girls, adolescents and persons of sexual and gender diversity and dissidence have the right to a life free of gender-based violence in all its manifestations, both in the public and private sphere, whether it comes from private individuals, institutions or agents of the State. The State shall adopt the necessary measures to eradicate all types of gender-based violence and the socio-cultural patterns that make it possible, acting with due diligence to prevent, investigate and punish it, as well as to provide care, protection and comprehensive reparation to the victims, especially considering the situations of vulnerability in which they may find themselves".
2. Constitution of Ecuador: Article 50.7: "The State shall adopt measures to ensure (...) protection against the influence of harmful programs or messages disseminated through any media that promote violence, racial or gender discrimination, or the adoption of false values".

3. Constitution of Kenya, Article 33(2): "The right to freedom of expression does not extend to the following manifestations: a. Propaganda for war, b. Incitement to violence, c. Hate speech, or d. Proselytizing of hatred that i. Constitutes incitement against an ethnic group, humiliation of others or incitement to cause harm, or ii. Is based on any ground of discrimination specified or referred to in Article 27(4)" (where sex is included).

Legislation examples:

1. Germany: 2017 law obliging platforms to remove potentially criminal content within 24 hours. The same law additionally obliges to remove "obviously illegal" speech, also within 24 hours, counting from the time the complaint is made.
2. Argentina: 2019 law that specifically punishes VPG, including sanctions such as prior warning, communication of the facts to the workplace of the "aggressor", or "mandatory attendance to reflective, educational or therapeutic programs aimed at modifying violent behavior".
3. Bosnia-Herzegovina: Law of 2006 prohibiting the use of any language, pictures, symbols, audios or videos that incite violence or spread hatred.
4. Spain:
    - Organic Law 1/2015, of March 30, amending the Penal Code: criminally punishes hate speech.
    - Law 15/2022, of 12 July, Integral Law for Equal Treatment and Non-Discrimination: requires public authorities to prevent and encourage the reporting of any type of violence and hate speech.

Relevant cases

Within the existing cases, we can differentiate between those that have given rise to administrative pronouncements and those that have given rise to judicial pronouncements.

Administrative pronouncement

1. Spain: complaint filed by the political party Plataforma per Catalunya (PxC) in 2015, against a self-proclaimed "anti-fascist" group, for publishing on the Internet that it defended national socialist and fascist ideology. The facts, in the opinion of the group, constituted an electoral crime. The Central Electoral Board, in Agreement 196/2015, of May 13, communicated that, in accordance with article 151 of the LOREG, it corresponds to the ordinary courts -and not to the Central Electoral Board- to determine the existence and authorship of the alleged crimes referred to by the formation.
2. Mexico:

a. TEPJF, Ruling SUP-REP-70/2021: VPG complaints must be processed in instance by the administrative electoral bodies (UTCE-INE).
b. TEPJF, Ruling SUP-REP-158/2020: confirms that the UTCE-INE are competent to process complaints for VPG and recalls that there must be a causal link between the allegation of alleged VPG and the material competence of such bodies.

Judicial pronouncement

Dozens of cases have been detected where the high courts of the same country (Mexico) have ruled specifically on the VPG. The pronouncements tend to protect women, as long as the facts and evidence allow it, legally speaking, although in other rulings the courts have tipped the balance against it. This should be food for thought, as it shows that transforming political ideology into law does not always work.

Outline of cases (all TEPJF):

1. Ruling SUP-REC-91/2020, where the issue of the lawfulness of a blacklist of persons committing VPG is discussed. The Court understands that this list is constitutional insofar as it is justified by the duty of public administrations to eradicate the VPG. The dissenting minority issued a harsh dissenting opinion in which it blamed its colleagues for "an inadequate inquisitorial judicial policy".
2. Ruling SUP-REC-61/2020, which distinguishes between so-called acts of political violence and acts of VPG and adds that if there is a complaint of VPG, those involved (all of them) must be personally notified within a maximum period of 48 hours.
3. Ruling SUP-JDC-156/2019, where the electoral administration is obliged to reevaluate a VPG complaint against a public servant who did not obtain redress.
4. Ruling SUP-REC-594/2019, where the VPG is put in relation to parliamentary inviolability. The decision on the merits states that the allegedly violent expressions are covered and that it would correspond to the Congress to sanction them. A dissenting opinion recalls that parliamentary inviolability is a matter of constitutionality, not legality.
5. Ruling SUP-REC-1388/2018, where the VPG poured in several Facebook videos is studied, the plaintiff is given the reason and a series of measures are included in the ruling to compensate the victim (publish in the press that she has been subjected to VPG and elaborate a protocol by the competent public administration to prevent and eradicate these behaviors).
6. Ruling SUP-REC-531/2018, which confirms the lawfulness of the annulment of an electoral candidacy due to the concurrence of VPG expressions.

Landmark cases:

1. TEPJF: Ruling SUP-REP-140/2020. VPG in its modality of digital violence. A candidate filed a complaint for the expressions used in a Facebook video. The Specialized Regional Chamber understood that such violence did indeed occur, even though the national legislation at that time did not sanction it, since several international, comparative law and even jurisprudential norms did. The minority of the High Chamber disagrees with the majority opinion due to its vagueness and imprecision.
2. TEPJF: Ruling SUP-JDC 111/2019, of July 3. It upholds the denounced man. He had posted a video and an article on Twitter criticizing the management of the leader, which he also published in various journalistic portals. The exact words were: (the leader) "destabilizes and divides the party"; she excludes from the candidacy people like him for being "critical of this cheating government"; that she "divides MORENA -the party- and that she should leave the presidency"; he compares her to Louis XIV and says that she "lost her compass".
3. TEPJF: Ruling SUP-REP27/2019. Candidate denounces VPG by men who spread an interview in social networks that does not leave her -she believes- in a good place. She bases her claim on the fact that the attack occurs "for the mere fact of being a woman". A man is sanctioned with more than eight thousand dollars but the High Chamber annuls it because her right to a fair trial was violated.
4. TEPJF: Ruling SUP-REP-623/2018. Candidate disseminates a video in social networks where another candidate is labeled as "Snow White Witch" and that, if you vote for her, you would be voting for her husband. The Specialized Regional Chamber understood that the stereotypes are discriminatory and, consequently, constitute VPG, an extreme that is confirmed by the High Chamber for "subordinating and minimizing the capacities of the candidate for political life".
5. TEPJF: Ruling SUP-REP-617/2018. Candidate denounced by VPG against another candidate because in a public discussion on Facebook this one told her: "I taught you how to work; poor thing, you are laughable and pitiful; unhappy and frustrated". In the first instance, the Specialized Regional Chamber considered such expressions as VPG. However, in the second instance, the High Chamber overturned this decision, understanding that the phrases did not constitute any unlawful act, taking into account both what was said and the context in which it was said, as well as the joint trajectory of the two, which ended in a row.
6. TEPJF; Ruling SUP-REP-121/2018 and Ruling SUP-REP-142/2018. Candidate denounces citizen for statements made on Facebook and in a blog that could constitute VPG. The electoral body issues precautionary measures

and orders the citizen to withdraw them. Faced with the refusal of the latter, he was fined, appealed before the jurisdiction that issued the referred resolutions, on the grounds that his right to freedom of expression was violated. The High Chamber confirmed the criteria of the INE and denied the plaintiff's right.

7. TEPJF; Ruling SUP-JDC-383/2017. Candidate denounces being subjected to VPG for the following expressions poured on social networks (especially Twitter): "Is Delfina a proper name? Or is that what they call her because of how she is treated by the one who appointed her and is her boss?". Second expression: "Puppet". Third expression: "Disaster of management as municipal president". Fourth expression: "Regrettable that a puppeteer wants to govern the State of Mexico". The High Chamber of the TEPJF ruled that the statements did not constitute GMV nor were they directed at the plaintiff because she was a woman, nor did they affect her in a disproportionate manner. Even if the acts were offensive, continues the resolution, that does not mean that it is political violence against someone. Furthermore, the Tribunal adds, in electoral processes, candidates should have more tolerance for harsh, harsh or strong criticism, since there is a greater general interest that is satisfied by freedom of expression and, especially in this case, freedom of information.

Critical conclusions

It is symptomatic and revealing that we do not even know what to call this "violence": gender violence, VPG, violence against women in politics, gender-based violence against women politicians. Closely related to such a diagnosis are two additional problems. On the one hand, no one knows what such violence really is from a legal perspective, but we do know that constitutional democracies are and were already equipped with a normative arsenal (including criminal) to combat certain things.

If by VPG we mean prohibiting any kind of ill-treatment, eradicating physical violence or, in short, preventing or attempting to compensate for any kind of legally intolerable harm to women (and men), the concept is inoperative because such conduct - and so much more - was already adequately covered and punished. Moreover, let us remember that human coexistence in freedom always involves nuisances and noises that provoke friction, disagreements, outrageous demonstrations, and other conditions derived from the *zoon politikon*. If the concept is not only not intended to "name" a reality but to build an ad hoc one, where women are kept in bubbles, treated as beings permanently in need of protection, and where it is assumed that words can hurt as much as actions, political violence based on gender will perpetuate what it wishes to combat, in addition to putting in the pillory, without solution of continuity, those it claims to want to protect at all costs.

On the other hand, freedom of expression as a fundamental right, even with the relevant limits, must prevail. We can never forget this: while free speech is a basilar

right that radiates all the others and finds a place in the best constitutionalist tradition, hate speech is a faint and misty notion created at the stroke of a sentence that, in the version we have studied here - the VPG - does not prove to be very operative. Even less so when it is brandished in political-electoral contexts where power is being fought tooth and nail. Exhausting libertarian reasoning, a certain degree of "strong" expression will always occur, since with freedom of expression we want to convince others of the goodness of what is ours, we want to provoke a clash of thoughts. VPG is very much like saying: give us a blank check and we (a few, the chosen few) will be in charge of managing the amount.

This question of VPG depends very much on the area, country, constitutional system (if there is any), regulation and respect for electoral norms, legal system, in short, so many variables that it is difficult to extract general rules, beyond this one: the denounced are men and the alleged victims are women. With mentalities like this, the idea is transferred, to give a lacerating example, that the men fallen in the fight against drug trafficking, countless, much less, than the women fallen in the same fight, a real problem because there are still brave men and women who defy the daily terror it imposes.

It should be added that gender is an abstruse, confused, variegated concept that no one agrees on, on the contrary, not even those who defend its validity and legitimacy. Some say it must be made central and others say it must be destroyed. Some say that thanks to gender, gender discrimination will be destroyed, and others even speak of erasing sex, as if attacking the most elementary biological nature of the human being were something from which one could emerge unscathed (as Macbeth said: "acts against nature engender disturbances against nature").

VI. Moderation In the Digital Space During the Electoral Period

María Garrote
Faculty of Law, Complutense University of Madrid
magarrot@ucm.es

The moderation function of digital platforms during the electoral period is, as we have seen, one of the nodes of the response to technological threats during the electoral campaign. Hence the need to focus on the risks that this function can generate, which, however, is absolutely necessary.

Internal content moderation procedures are a very important step forward in the fight against disinformation or the uncontrolled dissemination of political advertising or extreme political messages. However, these internal procedures generate mistrust and are not without risk. We can identify three major threats in the moderation function: First, they can become political censorship measures. The moderation of social media threatens freedom of expression and facilitates control over public opinion. It is not easy to identify what content is inappropriate, both in terms of the substance and the way it is disseminated, and in election periods, respect for freedom of expression must be maximized and equal opportunities must be guaranteed at all times. Secondly, digital platforms use algorithms to detect inappropriate content that may be biased. This algorithmic bias increases errors (which can have serious and irreversible repercussions on the electoral competition), reduces transparency and automates human bias. Finally, the decisions of social media platforms unfold in a framework outside of democratic control. The fundamental problem is that the regulation of content published on social networks is left in the hands of private companies, applying rules that are not of democratic origin and through technical mechanisms (based on algorithms) that lack transparency (Sánchez, 2020:119).

Glossary

The **moderation function** could be defined as the activity carried out by technology companies that own digital platforms or social networks in order to control the content published by users, which may even involve the removal of such content or the suspension of users' accounts. This control activity by companies affects two fundamental principles that should govern any electoral process: freedom of expression and equal opportunities for contestants.

In order to understand the scope of this function and the risks it may entail, it is necessary to refer to a series of technical terms related to this activity.

First of all, we should mention *algorithms*, which are intensively used by digital platforms and social networks to, among other things, compile and select the content that users see.

Algorithms are a finite set of formal rules (logical operations, instructions) that allow a computer to obtain a result from input elements. These rules can be subject to an *automated learning* process and have models designed through machine learning. Machine learning makes it possible to build a mathematical model to allow a computer to make decisions or predictions without human intervention based on the data, which include a large number of variables that are not known in advance. On the other hand, ***supervised learning*** is a form of machine learning that does not operate independently but requires human intervention. The data is presented to the machine and the process is guided by a person as the computer works towards a specific result. By, for example, labeling content, guided machine learning will generate an expected result.

The intensive and frequent use of algorithms leads us to another concept, ***algorithmic bias***: Technologies that do not consider the full range of available ideas and present repeatable errors in the output of a computer system, privileging one result over another. An algorithm may "program" a software so that it does not support a full range of inputs, but only a smaller spectrum. This bias is found in search engine results and social media platforms. This concept is linked to artificial intelligence and can also be described as digital manipulation of elections when an intermediary uses selective presentation of information to favor its agenda, rather than that of the users, who in this case are the voters.

Digital communications technology is the environment in which the moderation function will operate. It is the design and construction of communications technology that transmits information in digital form. These are digital tools that allow two or more people to communicate with each other. In this sense, ***digital literacy*** (information, media or information literacy) refers to the complementary and interwoven skills, both technical and social, that people must employ when using Internet-based communication (including hypertext, images, audio and video) to consume and create messages in a variety of academic, civic and cultural contexts. It is the literacy of emerging digital practices, where competent learners must perform equally well in face-to-face and print communication as new online tools. Related concepts are information literacy, information and communication technology (TIC, in Spanish) literacy, information literacy, media literacy, new literacies and multiliteracies.

In digital communication we encounter the phenomenon of "*cámaras de eco*" -**echo chambers**- In general, the term "echo chambers" illustrates the ways in which data bottlenecks or silos restrict the options available to people or machines. In social networks and other interactive platforms, where technologies often select snippets of data from a general source according to heuristics or learning algorithms, users may see a social network *feed* that becomes an "echo chamber" of similar or common ideas. An echo chamber can also be defined as a situation where people only hear opinions of one type or similar to their own. This means that other voices have been

actively excluded and discredited. Members of echo chambers have been led to systematically distrust all outside sources. In epistemic bubbles, other voices are not heard, while in echo chambers, other voices are actively undermined.

The ***Internet of Things*** (IoT) is the act of connecting any device with an on/off switch to the Internet (and/or to each other). This includes everything from cell phones, headsets, wearable devices, and even washing machines, etc. This also applies to machine components. The *IoT* is a giant network of connected "things" (which also includes people). The relationship is between people-people, people-things and things-things. It can be used or abused to change online political discourse by accessing and storing considerable amounts of personal or device user data and affect civic engagement online or in politics. Thus, *IoT botnets* are a network of *IoT*-connected devices that are infected with malware or controlled by malicious actors.

Ensuring a *level electoral playing field* must be a priority in any control or moderation activity in digital communication. A fair competition that ensures that every party and candidate is treated fairly and provided with exactly the same opportunities and financial resources, regardless of their size and popularity, ensuring them the same opportunity to make their case to voters. With the digitization of politics, this term can be used in relation to online political discourse, the use of social networks by wealthier candidates, etc. Directly related to this is the concept of ***net neutrality***, which stresses that Internet service providers must treat all data equally. Service providers cannot prioritize any data.

Cases

Regulation initiatives

For some years now, several regulatory initiatives have been put forward that, among other measures, seek to establish a series of guarantees in the moderation activity of digital platforms. At the state level, Germany passed a law on law enforcement in social networks (2017) that contains a series of measures to improve the effectiveness of laws and regulates the content removal procedure, which has not been without criticism. In addition, the Interstate *Treaty on Media* (2020) has an impact on the responsibility of internet intermediaries and imposes rules for the moderation function.

At the European level, the *Code of Conduct on disinformation* agreed by the European Commission in 2018 stands out - based on the report issued by a High Level Expert Group on Fake news and disinformation online - which is committed to self-regulation (the document was signed by Facebook, Google, Twitter, Mozilla and Microsoft) and transfers to companies the responsibility to intervene in content through a control that can be faster and more effective than that carried out by public authorities. Also in 2018, the Commission and the High Representative for Foreign Affairs and Security

Policy jointly adopted the Action *Plan against disinformation*, one of the pillars of which concerns the mobilization of the private sector through adherence to and compliance with the Code of Conduct.

Within the Council of Europe, the 2018 *Recommendation of the Committee of Ministers on the Role and Responsibility of Internet* Intermediaries reaffirms the obligation that any decision on content removal must be supported by a judicial authority or an independent authority, ultimately subject to judicial review, as well as other safeguards in the content removal process. The Venice Commission has compiled many initiatives into two must-have documents: a *report on Digital Technologies and Elections (2019) and Principles for a Fundamental Rights Compliant Use of Digital Technologies in Electoral Processes (2020).*

Relevant cases

There are several judicial and administrative precedents that have directly or indirectly addressed issues related to content moderation in digital communication.

Of particular interest is the Agreement of the Central Electoral Board of Spain that resolves the claim against Twitter for the suspension of the account of the political party VOX in that social network when the elections to the Parliament of Catalonia of February 14, 2021, were called. The suspension of the account, motivated by the publication of a message that contravened the policy regarding hate speech, was considered legitimate and proportionate. This agreement was ratified by the Supreme Tribunal in its ruling 246/2022 of February 28.

On February 6, 2022, the Superior Electoral Tribunal of Costa Rica resolved 63 cases in which it ordered the removal of content from social networks -during the electoral closed period- for violating the electoral legislation in Costa Rica regarding the prohibition of electoral propaganda. All contents were advertising and were hosted in the ad library. It proceeds to "order Meta Platforms, Inc. to immediately proceed with the removal of the advertising space".

The Electoral Tribunal of the Federal Judiciary of Mexico has resolved several cases on the publication of messages of non-candidates in social networks during the electoral ban and they have been considered electoral propaganda (the most recent, SUP-REP-319/2021. SUP-RAP-0172-2021 SRE-JE-0106-2021-Agreement 1).

In Brazil, there have also been relevant rulings in this area. The decision of the Superior Electoral Tribunal of May 2019 (Special Electoral Appeal No. 13351) indicates that messages sent through the Whatsapp application are not open to the public, as are those hosted on social networks such as Facebook and Instagram. The communication is of a private nature and is restricted to the interlocutors or to a limited group of people, which justifies, applying the proportionality canon in the strict sense,

the prevalence of freedom of expression. This interpretative line is reinforced in the decision of April 2020 (Recurso em Representação no. 060147858) in which it states that the carrying out of electoral propaganda on the profile of a legal person on the social network Facebook violates arts. 57-B and 57-C of Law 9.504/97 and entails the imposition of a fine.