İSTANBUL ÜNİVERSİTESİ YAYINEVİ

SİYASAL: Journal of Political Sciences, 32(1):15–33

DOI: 10.26650/siyasal.2023.32.1252061
http://jps.istanbul.edu.tr

Submitted: 16.02.2023
Accepted: 27.03.2023

SİYASAL: Journal of Political Sciences

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Social Networks and Democracy: Problems and Dilemmas of Regulating the Digital Ecosystem

José-Ignacio Torreblanca [1]

Abstract
The crisis of representative democracy is to a large extent a crisis of disintermediation. Its best known and most studied manifestation is expressed in the weakening of political parties and representative institutions and the link between them and the citizenry. However, the weakening of traditional media and the progressive replacement of their intermediary role between politics and citizens by social networks, although less studied, is of critical importance. This article analyses how the disintermediation of information facilitated by social networks aggravates the crisis of democracy. It shows how the characteristics of the digital ecosystem facilitate the spread of disinformation and fake news, erode citizens' trust in the veracity of information and contribute to the undermining of representative democracy and its institutions. It also examines the regulatory strategies being adopted by democratic governments to restore the quality of public space and public confidence in the media and the dilemmas and difficulties they face in doing so.

Keywords: Democracy, Social media, Mass Media, Disinformation, Fake News, Authoritarianism, Internet Governance, Freedom of Speech, Information-age, Public Sphere

1 **Corresponding Author:** José-Ignacio Torreblanca (Prof. Dr.) Department of Political Science, Faculty of Political Science and Sociology, UNED, Madrid, Spain. E-mail: jtorre@poli.uned.es ORCID: 0000-0002-9767-6239

To cite this article: Torreblanca, J. I. (2023). Social networks and democracy: problems and dilemmas of regulating the digital ecosystem. *SİYASAL: Journal of Political Sciences, 32*(1), 15–33. http://doi.org/10.26650/siyasal.2023.32.1252061

Introduction[1]

It is well known that representative democracy is undergoing a profound crisis. Freedom House (2022) and other relevant organisations have noted, in parallel to the rise of populism and authoritarianism, the worrying decline of democracy at the global level, a trend that is manifesting itself for the seventeenth consecutive year and is therefore structural rather than cyclical.

The facets of this democratic crisis are manifold and cannot be dealt with systematically here. It is important to note, however, its intimate connection with the technological change facilitated by the digital revolution. This transformation has a profound and lasting impact on a fundamental element of democracy: the functioning of the public space and, within it, the role of the media as intermediaries between citizens and political power.

This article aims to analyse the characteristics of the digital ecosystem that erode citizens' trust in the veracity of information and thus contribute to undermining democracy and its institutions. It aims to facilitate discussion on the regulatory options that legislators should consider protecting the general interest and rebuild a public and media space compatible with democratic principles and values.

The article has four sections. The first examines a lesser-known aspect of the crisis of representative democracy: the informational crisis that accompanies it. The second section details the characteristics of the digital ecosystem that increase the weakness and vulnerability of shared public space and representative institutions. The third outlines the reasons and ways in which authoritarian regimes exploit these vulnerabilities to interfere in democratic electoral processes and to undermine citizens' trust in democratic institutions and political forces. The fourth attributes these tensions to an extremely lax regulatory approach that has had adverse consequences both from a market (opening the way to monopolistic practices and situations) and political and social (weakening of the media and shared public space) point of view. To conclude, the different regulatory strategies adopted in the US and the European Union are examined, pointing out the markedly interventionist character of the latter as opposed to the US.

A Public Space in Crisis

Democracy is impossible without a shared public space. In that space there are facts and opinions. Information establishes the facts and deliberation allows for the exchange of arguments about the value and interpretation of those facts. In this public space, so-called "alternative facts", a crude but dangerous synonym for lies, are set against "raw facts". That is why it is said that citizens are entitled to their own opinions, but not their own facts. Without facts there is no possibility of debate, no possibility of establishing truth and no possibility of democracy (Arendt, 2017 [1967]).

In a small-scale democracy, such as the Greek one, the public space (the agora) can be face-to-face and governed by direct communication. But in a large-scale democracy, this is impossible. Because of their scale and complexity, contemporary democracies can only be indirect, or representative, democracies, which is why the crisis of representation

1 An earlier version of this article was published in Spanish in 2020 under the title "Democracia y redes sociales" in the Report "¿Cómo salvar las democracias liberales?" (How to save liberal democracies) published by Círculo de Empresarios.

they suffer is so important and central to the democratic crisis. Liberal democracy, with its checks and balances, separation of powers and rule of law, cannot be led just by assemblies. In fact, direct democracy has never guaranteed a quality deliberative public space, not even, as Socrates himself could testify, in Greece itself. Just as assemblies tended to be irrational even in Greek times and were easily manipulated by demagogues, contemporary experiments with direct democracy formulas have not generally fared any better (think, for example, of the Brexit referendum).

As we see daily, today's digital agora is very much like those chaotic assemblies, Greek or contemporary, where emotion easily prevails over reason and the most radical opinion displaces the most moderate. And it bears little resemblance to democratic parliaments, which over time have developed numerous institutional mechanisms designed to guarantee a certain stability of legislation: elections every four years, voting discipline, super-majority decision thresholds, constructive motions of censure, or specialised committees, among other mechanisms (Shepsle and Weingast, 1981).

While there was initially hope that the digital revolution would facilitate the transition to closer and more authentic direct democracy, this utopian dream has turned out to be false, and even dangerous. Digital democracy is technologically possible, but its political consequences can be devastating. Democracy requires, and will continue to require, intermediaries (political representatives) and, at the same time, the media, which are crucial for citizens to be able to know truthfully what their representatives are doing and thus to be able to control them effectively. Without reliable intermediaries, citizens cannot know the facts, establish the truth and thus control their rulers.

The problem is that technological change, as it has taken place over the last two decades, alters the ecosystem that allows representative democracy to exist. First, because it weakens the traditional intermediaries, the political parties, allowing citizens to coordinate more effectively to come up with alternative formulas for political participation and representation. This, which in principle should be welcome in that it allows citizens to break the oligopoly exercised by traditional parties, ends up proving problematic because the new parties or forms of participation that emerge, whether civic platforms or virtual communities, often fall into the same vices that they denounced and end up becoming plebiscitary parties dominated by hyper-leadership without internal plurality. All this is due to the same phenomenon experienced by the Greeks: disintermediation does not transfer sovereignty from the intermediaries to the grassroots, but to an even smaller and more difficult to control minority. The large technological platforms, after disintermediating the traditional media, have become closed monopolies that abuse their dominant position and prevent and block the progress of other companies (Lanier, 2018; López-Blanco, 2019; Soros, 2019).

The impact of digital disintermediation does not end with the weakening of political representation, but also has a powerful impact on the media, whose business model is weakened, making it impossible to finance quality journalism. It does so primarily through the diversion of audiences and consequent advertising revenues to digital platforms and social media. The European Commission has estimated that between 2010 and 2014 alone, the loss of revenue for print news publishers was €13.45 billion (European Commission 2018). These figures should come as no surprise as Facebook/Meta has 2 billion users,

YouTube 2.1 billion, WhatsApp 2 billion and Instagram 1.2 billion, and Tik Tok 1 billion. Out of a worldwide digital advertising market of $567 billion, Google and Facebook now account for 29% and 19%, respectively (Digiday, 2022).

As in the case of political parties, the crisis of the traditional media would not represent a problem if, as was envisaged at the beginning of this revolution, their digital substitutes could not only replace them in the fulfilment of this intermediation function, but even improve it, thus making it possible to overcome the shortcomings and errors of their analogue predecessors. The problem is that the new intermediaries, technological platforms and social networks, largely because of their own nature and business model, but also because of inadequate regulation, do not offer a re-intermediation that compensates for the disintermediation they cause, and therefore lack the necessary qualities to generate an alternative democratic public space to the one they destroy.

As evidence of this erosion of public trust, the Gallup Institute (Gallup and Kellogg Foundation 2019) found that between 2003 and 2016, the percentage of Americans who said they trusted the media fell from 54% to 32%. Most respondents identified inaccuracies and biases as the main factors behind their loss of trust in the media, to the point of placing it at the bottom of indicators of trust in democratic institutions (Ingram, 2018).

At the European level, things are not much different: according to Eurobarometer data, 68% of Europeans say they have been exposed one or more times a week to false or distorting information. Significantly, while 53% of Europeans still say they trust the press, only 24% say they trust the information they receive via social media and messaging platforms. The worrying result is that 82% of respondents say that fake news and misinformation are a problem for democracy (Eurobarometer 2018).

According to the Edelman Trust Barometer, which includes 26 countries, the problem is global in scope: put in order of their degree of trust in four key institutions - governments, businesses, NGOs and the media - the latter would be the worst rated institution of the four, enjoying the trust of only 47% of respondents, with only a worrying 36% trust in Spain (Edelman Trust Barometer, 2019).

The deterioration of that trust has led the London School of Economics to identify five major ills in British citizens' attitudes towards the public sphere and, consequently, to assert the existence of a "systemic information crisis that requires coordinated, long-term institutional responses" (Livingstone, 2019: 7). These five elements would be: "confusion", leading citizens to be unsure about what is true and what to believe; "cynicism", leading them to lose trust, even in authoritative sources; "fragmentation" of citizens into information niches where parallel realities and narratives exist; "irresponsibility", visible in the proliferation of organisations that operate both outside traditional ethical codes and outside control and accountability for their actions; and, finally, "apathy", manifested in a growing disaffection of citizens with the public sphere and a loss of faith in democracy and its institutions.

Risk Factors in the Digital Ecosystem

It is important to point out that the information crisis predates the digital era, as do the problems of democracy. Each wave of populism and democratic crisis has been

associated with an information crisis and a communication technology that has made it possible to disseminate the ideas of these movements. The press, which today we praise and whose demise we fear, played a major role in mobilising the first waves of populism that shook European democracies in the late 19th and early 20th centuries. It was also instrumental in instigating in European populations the nationalism that led to the Great War of 1914. As the British tabloids still show today, the tabloids never needed digital tools to sell its yellow journalism to the public. And the same can be said of radio, now considered a reputable medium, but which has been the indispensable companion of all totalitarianisms, from the 1930s to the most recent Rwandan genocide. And even books and the printing press, today sacralised as the highest forms of communication and culture, have historically played a very problematic role as instruments for spreading falsehoods, hateful ideologies, and disinformation. Recall how the biggest anti-Semitic propaganda operation, the one articulated around the false Protocols of the Elders of Zion, which claimed to prove the existence of a worldwide Jewish conspiracy, was prepared, printed, and disseminated by the Tsarist political police. Thus, the relationship between politics and communication technologies has always been complex. In that sense, although the digital revolution does not offer something new (the possibility of manipulating public opinion), it does offer something new and different (the possibility of doing so much more quickly and effectively).

There are several problems endogenous to social networks and digital platforms that make them highly problematic from the point of view of democracy. Disintermediation, already mentioned, is one of them. Also important is the business model, based on the so-called "attention economy", which revolves around the need to keep users on the platforms for as long as possible to expose them to as many advertisements as possible and to collect as much data on their behaviour as possible. The monetisation of attention requires prioritising emotions and the most controversial or eye-catching facts; in the case of politics, this involves amplifying negative or confrontational messages that deepen polarisation and generate traffic (Goldhaber, 1997; Gómez de Ágreda, 2019).

Another element is opacity. The algorithms that decide what takes precedence and what users of social media platforms and networks see first or most often are opaque. This means that users who want to appear in prominent positions on search engines or platforms have incentives to try to force the ranking system that companies use (the algorithms) in their favour. Most of the time this is done legitimately, i.e., by paying companies to achieve a better ranking, others by trying to understand how search engines work to optimise their posts for better rankings; sometimes by artificially and fraudulently generating traffic (Ghosh and Scott, 2018; Simpson and Conner, 2020).

A third problematic factor inherent to the digital ecosystem is the lack of adequate filters and controls, as networks are designed to facilitate access, not restrict it, making it easier for false information to pass as legitimate. In turn, the platforms' automatic advertising systems allow and encourage the creation of websites that appear to be legitimate media outlets but function as repositories and launderers of fraudulent information. These media pretend to be journalistic companies, but in reality, they are agents at the service of certain causes and political actors whose main task is to launder false information (Meleshevich and Schafer 2018). They usually establish and present themselves as local

media, as they are the ones, due to their proximity, that unsuspecting citizens are most likely to trust, and they generate traffic based on legitimate news (weather, sports, events or local information), which allows them to capture advertising revenue. On top of this content, they then add different layers of misinformation, for example, xenophobic or conspiratorial in nature (Yin *et al*, 2018).

In addition to the dissemination and re-dissemination of messages, true or false, by social networks on the basis of their algorithms, there is the presence of third party actors, who with advanced tools (fake accounts, bots) are able to create or amplify conversations, falsifying the image and perception that other users have of what is really happening and what is being said in the digital agora. For example, a study by Alto Analytics (2019) showed, after examining a total of 25 million movements on social networks (combining Facebook, Twitter, YouTube, Instagram and other digital communities), that 0.05% of users, who showed abnormal behaviours suggesting automation in the dissemination and re-dissemination of content, were responsible for at least 10% of the total political content generated during the Spanish European election campaign in May 2019. Similar studies by the same company have detected similar patterns of abnormal behaviour in phenomena such as the election of Jair Bolsonaro in Brazil, the yellow vest protests in France, or the anti-vaccine movements, among others.

The investigations into the Brexit referendum in June 2016, along with the US election in November 2016 that brought Trump to power, have given us a better understanding of how malicious actors have been able to exploit some of these features of social media to manipulate voters' sentiments and potentially guide their vote. Investigations by the FBI, the US Attorney's Office and independent experts have yielded solid and abundant evidence on the depth and extent of such interference. Operation Lakhta, coordinated from the Internet Research Agency, a huge troll farm based in St. Petersburg, published some 10 million fake tweets, 116,205 fake Instagram posts, 1,107 YouTube videos and 61,483 Facebook posts, reaching a combined audience of 126 million people in the US. This immense digital activity was not only important in quantitative terms but also qualitatively, as it was designed and targeted with very precise patterns of message segmentation by communities: the campaign encouraged right-wing voters to go out and vote through fake ads in which Muslim organisations invented in St. Petersburg but pretending to be based in the US called for a vote for Hillary ("Muslims for Hillary"). In other cases, the influence was aimed at reinforcing the African American community's feelings of pride and belonging (@blacklivesmatter) in order to demobilise their vote and get them not to support Hillary Clinton (SCSI, 2018; US vs Elena Aleekseevna Khusyaynova, 2018).

The micro-segmentation and disinformation tools used by the Kremlin converged with those used by the Trump campaign, directed by Steve Bannon, financed by Robert Mercer (who had also promoted Brexit) and designed by the Cambridge Analytica company, directed by Alexander Nix, which brought together the best experts in psychometric techniques, i.e., designed to understand and manipulate the emotions of voters. One of these techniques, called OCEAN, used five concepts: "openness" to experience, "conscientiousness", "extraversion", "agreeableness", and "neuroticism" to construct personality profiles. This research was then transferred to the experimental level, where, via focus groups with groups of potential voters, an attempt was made to understand how

negative political emotions functioned and were instigated. SCL, Cambridge Analytica's campaigning company, boasted to its clients that it had profiled 240 million Americans, with between four and five thousand pieces of data on each of them (Confessore and Hakim, 2017; Wylie, 2019).

The ease with which it was possible to present distorted information or manipulate emotions and influence the voting intentions of millions of Americans was not only due to the lack of scruples of some companies or businessmen but also to the simplicity with which these companies were able, thanks to their collaboration with digital platforms such as Facebook, to appropriate the personal data of 87 million Americans to use them for fraudulent political purposes. In this way, they gained invaluable voter information that other political campaign operators and polling companies lacked, allowing them to target their campaign resources and messages to 13.5 million potential voters in sixteen key states in the American Midwest that traditional companies had previously ignored for lack of accurate data and profiles (Persily, 2017).

It has been estimated that the combined impact of these actions resulted in 25% of Americans being exposed to some form of fake news during the height of the election campaign (October-November 2016), but with a very significant incidence among conservative voters: 6 out of 10 visits to these fake news repositories were concentrated among the top 10% of conservative voters (Guess *et al*, 2018). Moreover, older people were the most vulnerable: those aged 65 and over were five times more likely to share fake news than those aged 18-25 (Barberá, 2018; Howard *et al*, 2019).

Although companies such as Facebook have repeatedly denied offering their customers products based on information about their users' emotional states, there is sufficient evidence that their staff have done so (Levin, 2017). More seriously, Facebook has not only collected emotional information, but experimented with how to create or manipulate those emotions (Garcia-Martinez, 2017). The ultimate goal of all this research, commercial in its origin, was to offer advertisers the possibility to reach their potential consumers with a precision never known before, even in a predictive way, i.e., to be able to predict from consumers' activity on social networks at what point a consumer was planning or predisposed to purchase a consumer item (Biddle, 2018).

In the political arena, Facebook researchers have also successfully experimented with techniques to increase voter turnout based on social pressure from the voter's immediate environment: in the 2010 congressional elections, it mobilised an additional 340,000 voters in an experiment involving 61 million users (Bond *et al*, 2012; Corbyn, 2012). It has also done research on how to influence the political opinions and votes of people using its platform based on the order of presentation and sequence of presentation of information about a candidate or party or according to theories of 'emotional contagion' (Kramer *et al*, 2014).

As Soshana Zuboff (2020) has warned, for years users thought they were using Google as a search engine when the reality was that Google was the instrument for searching them. It was therefore just a matter of moving the research that the platforms themselves were already doing on the emotional predispositions of their users from the consumer to the political level (Christl *et al*, 2017). Given the immense volume of personal information

collected by platforms without users' knowledge and for marketing and advertising purposes, it was only a matter of time before this information was used for electoral purposes. As Emma Briant (2018) has pointed out, advances in propaganda techniques that combine the illegal extraction of personal data with the use of artificial intelligence tools and knowledge derived from neuroscience and psychology are far ahead of our knowledge and, consequently, our ability to regulate.

Foreign Interference in Democracies

Although important, election interference represents only a small part of the disinformation problem: its scope and depth have made it a major global problem. Freedom of the Net (2019) identifies as many as 30 governments that produce and disseminate content to distort information circulating on the internet, with particular emphasis on Russia, China, Iran and Saudi Arabia.

As we have seen during the COVID-19 crisis, information has become an additional field of geopolitical friction between authoritarian regimes and liberal democracies (Rosenberger and Howard, 2020). In the Russian case, through increased actions aimed at sowing confusion and mistrust in scientists and politicians. And in the Chinese case, through a strategy aimed at covering up the damage that the initial origin and concealment of the virus has done to its international image (Cardinal, 2020; East Stratcom Task Force, 2020). This strategy has had two elements of action: one positive or friendly, consisting of using social networks to amplify the image of Chinese generosity and the corresponding gratitude; the other, more aggressive, aimed at sowing information that reinforces the theory that the virus may not have originated in China or attacking those who criticise China. An example of this first strategy is the study by Formiche magazine of the 47,821 tweets by the Chinese Embassy in Rome in February 2020 showing photographs of planes carrying Chinese medical equipment to help in the COVID-19 crisis: the study concluded that 46.3% of these tweets, under the hashtag China with Italy (#forzaCinaeItalia), showed automated patterns of behaviour and therefore sought to artificially create the appearance of spontaneous solidarity between China and Italy (Carrer and Bechis, 2020).

That both Moscow and Beijing are the actors that most systematically employ disinformation is neither coincidental nor confined to the COVID issue: in fact, they do so strategically. There are two reasons for this. First, for authoritarian regimes, control of information is an existential necessity: just as democracies cannot survive without free media and informed citizens, dictatorships cannot coexist with freedom of information without a crisis. Therefore, even if they did not need them to sustain themselves internationally, it would still be essential to have and practice such propaganda and disinformation strategies inwards, which gives them experience and repertoires of action in this area (Sanovich, 2017).

Second, if, as is the case, these regimes also live in a hostile geopolitical environment, outside information is essential in two different ways: first, passive, insofar as they need to block or filter their citizens' access to truthful information from abroad; second, proactive or offensive, which consists of weakening their enemies. The latter strategy, which consists of disseminating false or malicious information that diminishes the enemy's self-confidence and thus its willingness and ability to confront, has dominated

the geopolitical landscape of Russia-West relations over the past decade. According to the European Parliament, information warfare strategies operate on two fronts: one, cybersecurity, where the aim is to damage the opponent's information infrastructures; and two, psychological, where the aim is to influence the enemy's population and/or its leaders to make decisions favourable to the opponent's interests (European Parliament Research Service, 2015).

In the case of Russia, the consistency and perseverance of its disinformation strategies is, paradoxically, related to its weakness. Since coming to power in 2000, Putin's goal has been, to use Trump's frame of mind, to 'make Russia great again'. However, despite its vast natural resources and the availability of a large armed forces, including nuclear weapons, Russia's leaders are aware that the West's power is far superior economically and militarily - its GDP is lower than France's and its military spending is a fraction of that of the US and Europe.

Yet, as the dissolution of the USSR and the Warsaw Pact showed at the time and the so-called 'colour revolutions' on Russia's borders have demonstrated, far more threatening than the West's military might is the attractiveness of its model of life to its citizens. This factor, which Joseph Nye has described as "soft power", refers to the attractiveness and influence that open, prosperous, and free societies exert on those that are not (Nye 2005). In the case of Russia, the extension to its borders of the number of free and democratic states that have looked to the Atlantic Alliance, rather than Moscow, for their security guarantees has been interpreted in Moscow as a threat to the survival of Putin's political model. From the secession of Kosovo, a dangerous precedent for a federal country with large Muslim minorities, to the Orange Revolution in Ukraine, a country that Russian nationalist elites see as inextricably linked to Russia, to the pro-democracy protests in Russia in December 2010, which Putin has always seen as US-instigated, it has been clear to the Russian regime that its survival depended on weakening the appeal of the Western model of life, both to its own citizens and to Western citizens themselves. This has led to a strategy of reinforcing the verticality of power within Russia, terrorising or putting heavy pressure on dissidents but, above all, imposing an iron grip on the media, especially television. And, in parallel, an external strategy aimed at promoting Westerners' distrust of their democratic institutions and, especially, providing information support to the anti-establishment forces that in each country, from the National Front in France to Alternative for Germany or the League in Italy, were most likely to bring to power populist anti-European parties that would weaken both intra-European cohesion and the transatlantic link (Milosevich, 2017).

It is in this context that Russian state media (Sputnik or Russia Today) aimed at foreign audiences are born and operate. As US Secretary of Defence General Mattis (2005) pointed out in 2005, the overwhelming US military superiority forces its enemies to renounce conventional warfare and forces them instead to seek niches of irregular confrontation where the combination of technology and other opportunistic tactics allows them to gain an advantage, a strategy confirmed by Russian strategists in their numerous pronouncements on hybrid warfare and their actions abroad, from Crimea to Salisbury (Ng and Rumer, 2019). The strategy is also confirmed by the heads of Russian state media, such as Margarita Simonyan, director general of Russia Today, who in 2013 confessed

in an interview that in 'peacetime an international channel would not be necessary, but in wartime it can be crucial' (Resinger and Golts, 2014; Rutenberg, 2017). Since then, whether it is the idea that the European Union has no future, that the far right is spreading across Europe, encouraging xenophobic movements, campaigns against George Soros, lies about the downing of MH-17 over Ukrainian territory or vaccines, these state media have exploited all the weaknesses they have found in Western democracies, including, in the Spanish case, the secession of Catalonia (Alandete, 2018; Polyakova *et al*, 2017).

Disinformation not only weakens democracies but, in parallel, strengthens authoritarian regimes. Authoritarian regimes have not only mastered social media on the international front to discredit democracies in the eyes of their citizens and their own, but at home to strengthen their regimes in hitherto unthinkable ways. What were once mass media and totalitarian propaganda tools have today become mass surveillance tools thanks to the combination of artificial intelligence tools that allow them to collect and exploit data to politically profile their citizens to control them more closely. In the Chinese case, the use of such techniques, combined with facial recognition, has degenerated into an authoritarian techno-nightmare of major proportions and put the Chinese regime in a position to achieve the dream of every authoritarian regime: to be able not only to detect dissidents before they organise themselves but, using artificial intelligence tools, to predict who they might potentially be (Human Rights Watch, 2019; Soros, 2019).

The Internet was born out of a utopian dream of global liberation and universal knowledge. But the reality today is that of the 3.8 billion people who have access to the internet, 71% live in countries where they can be fined or imprisoned for expressing their political opinions or religious feelings on the internet and 56% in countries where the authorities block content for ideological reasons. In fact, only 20% of internet users live in countries considered free and only 7% of countries that hold competitive elections are free from electoral interference (Freedom on the Net, 2019).

The owners of Cambridge Analytica claimed to their clients that their technicians needed only 70 likes from a Facebook user to know more about that person than their friends, 150 to know more than their parents and 300 to know more than their partner. Above that number, they presumed, they already knew more about that person than the person themselves (Illing, 2018). A claim intended to prove the commercial potential of their apps, which allowed them to promise a phone or insurance company that they could predict when a user was going to request a transfer or unsubscribe, but which in a context such as China's takes on a very threatening meaning from the point of view of human rights and the possibility of political change. And it highlights the extent to which malicious use of the digital ecosystem is intimately linked to the very characteristics of that ecosystem.

Regulatory Options and Models

The dire consequences of the deregulation of social platforms and networks in terms of the functioning of markets, increasingly dominated by the monopolistic practices of a few companies, and its debilitating impact on democracies and their representative institutions, is generating a convergence in terms of regulatory preferences. It is remarkable, for example, that one of the fathers of the Internet, Tim Berners-Lee (2014), and a renowned

sociologist such as Anthony Giddens (2018) agree on the need to enact a Digital Bill of Rights to complement the classic declarations of rights. Gone is the well-meaning utopianism that presided over the beginnings of the digital revolution, visible in John Perry Barlow's 1996 Declaration of Independence of Cyberspace: "We are creating a world in which everyone will be able to participate without privilege or prejudice created by race, economic or military power or place of birth, a world where everyone will be able to express their beliefs, whatever they may be, without fear of being coerced or silenced" (quoted in Persily, 2019).

Statements like that reflect well the spirit that dominated internet regulation in its early days. That same year, 1996, saw the enactment of the US Communications Decency Act, a law that today virtually all observers place at the root of the problems of accountability of social media platforms and networks for the content they publish. In section 230, section C.1, the US Congress established that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". In this way, it provided immunity to technology companies, but also to the authors of blogs or any other type of pages, against content posted by third party users that could eventually be considered defamatory or offensive by the courts. This law provided legal cover for users of YouTube, Vimeo, Facebook or Twitter to post their content on these platforms without being obliged to view their content beforehand or authorise its publication. Its aim was to preserve freedom of expression, as review was considered a form of censorship, and to allow for growth and innovation in the sector, something it certainly achieved. In practice, however, it turned technology platforms into "noticeboards" exempt, except in a very small number of cases, from liability for their content.

One of the main criticisms of this law today is that it ignores the fact that these companies were always much more than neutral repositories where users hosted their content: in practice they have been and are active agents that order, prioritise and re-distribute this content to monetise it through the sale of advertising, which in practice makes them publishers of this content. The media emerged with the purpose of serving that purpose of conveying truthful information and were regulated accordingly to ensure that they did so and to punish those who failed in that duty. Social media, by contrast, were not born to inform, a job that requires editors, hierarchy, barriers to access, regulation, control, and courts to bring the media before to force them to rectify, but for people to share their life experiences horizontally on a massive and immediate scale. The paradox is that, as happened in the case of other digital platforms, such as Uber, they were not regulated at the beginning either by the service they provided (transporting passengers) or by the legislation of the sector of what the companies claimed they were (communication platforms), remaining in a kind of legal limbo in which they largely remain today.

From the well-meaning utopian thinking that was at the origin of social networks, which, in a kind of global Athenian agora, affirmed the creation of new spaces of freedom and collective democracy based on direct communication between citizens, we have moved on to a much more pessimistic view of the compatibility of democracy and social networks. Unsurprisingly, once the economic and commercial fabric that underpins the free nature of these enterprises, not to mention their permeability to capture by foreign

agents and powers, has been exposed, discourses about the global agora, the birth of a global consciousness and what Zuckerberg has called the "fifth estate" have lost all their appeal (Thornhill, 2020). If malicious action by authoritarian states is possible, it is largely due to the failure of democracies to adequately regulate social networks (Freedom of the Net, 2019). An entirely new regulatory approach to the problem, one based on the duty of care of platforms, is needed, experts argue (Perrin, 2020).

Such regulation is something that the EU is able to do successfully, even to lead globally. The differences between the US and EU regulatory cultures are stark. The European Commission has successfully intervened in the privacy framework with a regulation, the General Data Protection Regulation (GDPR) (European Union, 2016, which has been a turning point for large technology companies, which have been forced to adopt much higher privacy standards than those they must observe in the US. In other fields as well, such as copyright, artificial intelligence, child protection, the right to be forgotten or disinformation, the EU has shown a clear capacity to become a regulator and creator of global standards, which has led some to characterise it as a "regulatory superpower" (Bradford, 2020).

To date, the US government and Congress have shown little capacity or interest in confronting its technology industry, which contributes substantially to its global power and economic well-being, as well as to campaign finance. For its part, China seeks to recreate its own local Silicon Valley to exploit to the full the capacity of these technologies to exert social control and thus sustain the CCP-led authoritarian regime through a suffocating layer of digital technology. We have seen, however, how in recent times the investigations and sanctions by European competition authorities into abuses of dominant positions or irregular practices by these large companies have begun to open a crack in the US legal system, empowering activists whose regulatory theses are closer to Europe's positions (Burnell, 2018).

With regard to China, although the EU has watched with great frustration as the new great Chinese digital wall has grown beyond the regulatory reach of Europe, and also of European technology companies, which are excluded or discriminated against in the Chinese market, we have seen the awakening of a new awareness in Europe of the need to ensure that Chinese companies operating on European territory comply with European standards in terms of data protection and also positioning in terms of critical infrastructures. Here too, COVID-19 has provided a new awakening by highlighting how the mobile applications that are essential for an orderly and successful exit from the pandemic may represent a new twist in the ability of states (China) or companies (US) to further intrude on people's privacy (Ghosh, *et al* 2020; Simpson and Conner, 2020).

In the specific field of disinformation, the European Commission has decided to consider it a threat to democracy, public policy, citizens' security, public health, and the environment, and to take action accordingly. The Commission's Communication on the issue, adopted in April 2018, under the title "Combating online disinformation: a European approach", defines disinformation as "verifiably false or misleading information which is created, presented and disseminated for profit or to deliberately mislead the public, and which is likely to cause public harm". Disinformation, the Commission argues, "erodes trust in institutions and in digital and traditional media and damages our democracies by

hampering citizens' ability to make informed choices, supports radical and extremist ideas and activities, and undermines freedom of expression" (European Commission, 2018).

The Commission's approach is that disinformation is not an accidental product or an unintended consequence of freedom of expression on social media. Both those who create it and those who collaborate in its dissemination are responsible for it. Among the former, the Commission points to "a range of domestic and foreign actors using mass disinformation campaigns to sow mistrust and create social tensions, which can have serious consequences for our security", and can also be part of "hybrid threats to internal security, including electoral processes, especially when combined with cyber-attacks". The latter include "social networks, video-sharing services and search engines, which play a key role in spreading and amplifying disinformation online" as they have not only "failed to take proportionate action or address the challenge posed by disinformation and manipulative use of platform infrastructures" but have also failed to allay suspicions that the personal data of millions of users is sufficiently protected against unauthorised use for electoral purposes by third parties.

Hence, the European Commission rightly considers that the problem goes far beyond fake news. Indeed, to the extent that it diverts attention from the main problem and minimises it, the focus on fake news can be counterproductive. Certainly, news verification is an important element in any kind of strategy against disinformation, but it cannot be the only one, nor will it be effective if it ignores that the problem is not just fake news, but fake media, fake users and, above all, that the problem does not originate in politicians failing to tell the truth, but in society ceasing to believe in the possibility of truth. The problems and controversies surrounding verification companies, many of them funded by platforms such as Facebook, have rightly highlighted the limits of the verification strategy. As we have seen, verifying that a Trump statement is false then requires, as Twitter has recently done, the courage to label that statement as false or malicious, or remove it because it glorifies violence.

The translation of this regulatory challenge into actions is very revealing. After intense negotiations by the European Commission with tech companies, they have been forced to adopt a code of conduct that obliges them to monitor fake profiles and accounts and report regularly on their actions. The results are very illustrative and show that the scale of the problem is even greater than previously thought. In just the first two months of active scrutiny of its own platform activities in 2018, Facebook identified 600,000 fraudulent or inappropriate ads. Google, meanwhile, revealed that between September 2018 and August 2019 it had taken 314,288 actions against ads served on its own platform. Microsoft also provided surprising data, reporting that it had removed 900 million ads. As for fraudulent profiles and fake accounts, Facebook, which does not provide information on the total number of accounts, only statistics on users, says it deactivated 2.19 billion fake accounts in the first quarter of 2019, identifying at least 7,606 accounts to which it attributed "coordinated disinformation actions". Twitter, meanwhile, terminated 126 million accounts and YouTube did the same with 10 million channels to which it attributed fraudulent or inappropriate content. The magnitude of these data reveals the extent of the problem of laxity and lack of control by poorly or inadequately regulated companies (European Commission, 2019).

The European Commission is therefore right when it argues that combatting disinformation requires, in addition to the promotion of education and media literacy, a more transparent and accountable ecosystem, as this is the only way for citizens to regain trust in. As Persily (2018) points out, actions should encompass a broad panoply of measures: erasure, relegation, disclosure, delay, dilution, diversion, deterrence and education. Internationally, foreign policy.

In addition to the European Commission, many European states have taken or are considering taking measures against disinformation. But fighting disinformation is not easy. As in so many other regulatory areas, it is easier to point out what should be avoided than to design a catalogue of actions that would radically eliminate the problem, especially when, as has been said, the problem is the ecosystem itself. The German government, for example, has opted for a strategy of fining internet platforms that do not eradicate content reported and verified as false or hate speech. France, on the other hand, has preferred to focus on judicial control of platform content (Colomina, 2019).

Underlying the disagreements between the US and the EU, which are undoubtedly business and geopolitical, are important differences in political and legal cultures. The First Amendment of the US Constitution restricts the possibility of limiting freedom of expression in a much more restrictive manner than is established in European legislation, where the regulation of hate speech allows for a wider range of measures and legal actions against platforms and users (García Morales, 2020). In the European case, we have even seen a ruling by the Court of Justice of the EU in which it held that political propaganda in the event of a military conflict is not guaranteed by freedom of expression, thus validating the restrictions imposed on the official Russian news agency to report on the Ukrainian conflict in the territory of the EU (Hanley, 2020).

At one extreme, citizens' trust in democracy and even democracy itself is at stake. At the other is freedom of expression, whose limits must be as narrow as they are clear. In the middle are technology companies, faced with a new citizen awareness and legislators who have lost their technological innocence and are moving towards regulation that they see both as a threat to their business and as worrying from the point of view of legal security. Platforms' lives, once comfortable and dominated by steady growth in revenue and users, are now dominated by concerns about the sustainability of their business. Even after hiring thousands of people to monitor what their users post, platforms do not see themselves capable of ensuring that the content that remains on their walls complies with the law (Hobbs, 2019). And they are right, because if in the same country, as is the case in Spain, two courts can rule completely differently in two similar cases on the content of expressions posted online, imagine the challenge this poses when the network is global, and what a judge in the US may consider protected by freedom of expression in Germany constitutes a crime classified as hate speech.

An additional problem with regulation is that of effectiveness. Any measure of control or prohibition forces an adaptation of the opponent: what is true for those who design fighter planes that fly under the radar is also true for the perpetrators of disinformation. The regulation and limitation of visible content on Facebook and Twitter has already had the unintended consequence of encouraging the migration of much toxic content to networks such as WhatsApp, where the dissemination can be equally or even more

viral but much more difficult to detect and control, or to alternative closed platforms, such as gab.ai, the platform of the US far right (very popular in the 2018 Brazilian election), where it is preached that there is no censorship but total freedom of expression to upload content that in reality is pure hate. As evidenced by advances in the production of deep fakes, technology will always be ahead of the regulator, especially in the realm of the illicit, which means that governments can easily end up in the worst of all worlds: sacrificing freedom without achieving security. But that is the world they must navigate: however uncomfortable, difficult and fraught with contradictions, it will always be far better than the dissonance between some people's certainty of living in a utopia of global connectedness in freedom and others' certainty of being trapped in a dystopian technological nightmare. As many of the initiatives taken by companies to better regulate the sector globally and rebuild trust demonstrate, that road has already begun to be travelled (Paris Call, 2019; Zuckerberg, 2019).

Finally, we cannot ignore the fact that, alongside the problems of disinformation supply, there are also problems of demand, ranging from the psychological and cognitive predispositions of people to receive and disseminate this type of information to those related to a lack of political or informational culture, which therefore also require educational interventions that, in a democracy, are necessarily difficult (Jackson, 2018; Jeangéne *et al.*, 2018).

Conclusion

Disinformation poses a threat to democracy. But as with almost all threats to democracies, responses to them will always be limited in scope and effectiveness by the need, in their right to self-defence, not to harm themselves and their values more than their enemies do. In the fight against disinformation, democracies operate with one hand tied behind their backs, almost both. Because the dispute over truth is part of the democratic discussion, shielding the truth is neither possible nor desirable: it is directly counterproductive and incompatible with democracy (Arias Maldonado, 2017). Democracies, it has been said, must fear both their own and foreign powers (Innerarity and Colomina, 2020). Limitations on freedom of expression, while justified, will of necessity always be imperfect and incomplete.

The dilemma is clear: leaving the censorship of tech companies' content in the hands of governments is as bad an idea as leaving it in the hands of the companies themselves. In turn, the absence of limits on content not only damages the democratic public space and makes it permeable to misinformation, both from local and foreign actors, eroding citizens' trust in their institutions and values, but can also harm individuals and rights in substantial ways.

The EU and member states are therefore faced with the need to act in different ways at different levels. At the international level, they seek to act firmly against actors who use disinformation as a weapon of war to undermine democracies, while leading a global regulatory response based on the universal principles and values that underpin representative democracy, human rights and a rules-based multilateral liberal order that is highly beneficial to Europe. At the domestic level, by contrast, while protecting users from the most serious and obvious online harms that violate their fundamental rights,

they seek a constructive and careful approach to achieve (through a three-way alliance between governments, business and citizens based on dialogue and experimentation), build and sustain a quality public space and media that bring proven facts to public debate rather than polarisation and undermining of democratic institutions.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

References

Alandete, D. (2019). *Fake News: la nueva arma de destrucción masiva*. Madrid: Deusto.
Alto Analytics (2019). Spain: Digital Public Debate Ahead of EU Parliamentary Elections. [Web log post]. Retrieved from: https://www.alto-analytics.com/en_US/blog/
Arendt, H. (2017) [1967]. *Verdad y mentira en la política*. Madrid: Página Indómita.
Arias Maldonado, M. (2017). Informe sobre ciegos: genealogía de la posverdad. In J. Ibáñez (Ed.), *La era de la posverdad* (pp.65-67). Madrid: Criterios.
Barberá, P. (2018). Explaining the spread of misinformation on social media: Evidence from the 2016 US presidential election. Symposium: Fake News and the Politics of Misinformation. APSA Comparative Politics Newsletter. Retrieved from: http://pablobarbera.com/static/barbera-CP-note.pdf
Biddle, S. (2018, April 13). Facebook uses artificial intelligence to predict your future actions for advertisers, says confidential document. *The Intercept*. Retrieved from: https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/
Berners-Lee, T. (2014, May 28). Necesitamos una Carta Magna para Internet. *El País*. Retrieved from: https://elpais.com/elpais/2014/05/14/opinion/1400069758_586516.html
Bond, R., Fariss, C., Jones, J., Kramer A., Marlow, C., Settle, J., and Fowler, H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature,* Letter, (489), 295-298. Retrieved from: https://www.nature.com/articles/nature11421.
Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.
Briant, E.L. (2018). Three Explanatory Essays Giving Context and Analysis to Submitted Evidence. Retrieved from: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Dr-Emma-Briant-Explanatory-Essays.pdf
Burnell, F.G. (2018). Making America First in the Digital Economy: the Case for Engaging Europe. *The Atlantic Council*. Retrieved from: https://www.atlanticcouncil.org/wp-content/uploads/2018/05/Digital_Economy_WEB.pdf
Cardenal, J.P. (2020). Propaganda china para un escenario post Covid-19. *Centro para la Apertura y el Desarrollo de América Latina*. Retrieved from: https://www.cadal.org/publicaciones/informes/?id=12779
Carrer, G. and Bechis. F. (2020, March 30). Così la Cina fa propaganda in Italia, con i bot. Ecco l'analisi su Twitter di Alkemy per Formiche. *Formiche***.** Retrieved from: https://formiche.net/2020/03/cina-propaganda-twitter-bot-alkemy/
Colomina, C. (2019). La desinformación de nueva generación. *Anuario Internacional CIDOB* 61-66.
Confessore, N., and Hakim, D. (2017, March 6). Data firm says 'secret sauce' aided Trump; many scoff. *The New York Times*. Retrieved from: https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html
Corbyn, Z. (2012). Facebook experiment boosts US voter turnout. *Nature, News and Comment* No. 12. Retrieved from: https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401
Christl, W., Katharina, K., and Riechert, P.U, (2017). Corporate surveillance in everyday life. Cracked Labs: 6.
Digiday Editors (2022). Here are the 2022 global media rankings by ad spend: Google, Facebook remain dominant — Alibaba, ByteDance in the mix. Retrieved from: https://digiday.com/?p=480387
East Stratcom Task Force, (2020). EEAS Special Report Update: Short Assessment of Narratives and Disinformation around the COVID-19 Pandemic. Retrieved from: https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/
Edelman Trust Barometer (2019). 19th Annual Edelman Trust Barometer Global Report". Retrieved from: https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report.pdf
Eurobarometer (2018). Fake news and disinformation online". Flash Eurobarometer 464. Retrieved from: https://op.europa.eu/en/publication-detail/-/publication/2d79b85a-4cea-11e8-be1d-01aa75ed71a1
European Commission (2018). Tackling online disinformation: a European Approach", Communication from

the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

European Commission (2019). Code of practice on disinformation: first annual reports - October 2019. European Commission.

European Parliament Research Service (2015). Understanding propaganda and disinformation". European Parliament. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571332/EPRS_ATA(2015)571332_EN.pdf

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. OJ-L-119 of 4 May 2016. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Freedom of the Net (2019). The Crisis of Social Media. Retrieved from: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

Freedom House (2022). Freedom in the world 2022: The Global Expansion of Democratic Rule. Retrieved from: https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

Gallup and Knight Foundation (2018). Indicators of news media trust: Retrieved from: https://knightfoundation.org/reports/indicators-of-news-media-trust/

Garcia-Martínez, A. (2017, May 2). I'm an ex-Facebook exec: don't believe what they tell you about ads. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2017/may/02/facebook-executive-advertising-data-comment

García Morales, V. (2020). Donde habitan las mentiras: libertades de expresión e información en tiempos de odio e hiperinformación. *Revista CIDOB d'Afers Internacionals*, (124) 25-48. http://doi.org/10.24241/rcai.2020.124.1.25

Ghebreyesus, T.A. (2020). Speech delivered at the Munich Security Conference on 15 February 2020, World Health Organization, Coronavirus disease 2019 (COVID-1) Situation Report (85) p.2. Retrieved from: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200415-sitrep-86-covid-19.pdf?sfvrsn=c615ea20_4

Giddens, A. (2018, May 6). Una Carta Magna para la era digital. *La Vanguardia*. Retrieved from: https://www.lavanguardia.com/vida/20180506/443286426188/una-carta-magna-para-la-era-digital.html.

Ghosh, D. and Scott, B. (2018). Digital Deceit: The Technologies Behind Precision Propaganda on the Internet. *Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy*. Retrieved from: http://medienorge.uib.no/files/Eksterne_pub/digital-deceit-final-update1.pdf.

Ghosh, D., Abecassis, A., and Loveridge, J. (2020). Privacy and the Pandemic: Time for a Digital Bill of Rights. *Foreign Policy*. Retrieved from: https://foreignpolicy.com/2020/04/20/coronavirus-pandemic-privacy-digital-rights-democracy/

Goldhaber, M. H. (1997). The attention economy and the net. *First Monday* (2) No. 4 - 7. Retrieved from: https://firstmonday.org/ojs/index.php/fm/article/download/519/440

Gómez De Ágreda, Á. (2019). *Mundo Orwell: Manual de supervivencia para un mundo hiperconectado*. Barcelona: Ariel.

Guess, A., Lyons, B., Montgomery, J.M., Nyhan, B., and Reifler, J. (2018). Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 US midterm election campaign. Hanover: Dartmouth College. Retrieved from: https://www.dartmouth.edu/~nyhan/fake-news-2018.pdf.

Hanley, M., (2020). Salvaguardar el espacio informativo: las políticas de la UE y Ucrania ante la desinformación. *Revista CIDOB d'Afers Internacionals* (124) 73-98. http://doi.org/10.24241/rcai.2020.124.1.73

Hobbs, C. (2019). Can regulation save the Internet: The view from London. Commentary *European Council on Foreign Relations*. Retrieved from: https://www.ecfr.eu/article/commentary_can_regulation_save_the_internet_the_view_from_london

Howard, P., Ganesh, B., Liotsiou, D., Kelly, J., and François, C. (2019). The IRA, social media and political polarization in the United States, 2012-2018. Project on Computational Propaganda. Retrieved from: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

Human Rights Watch (2019). China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App. Retrieved from: https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

Illing, S. (2018, April 8). Cambridge Analytica, the shady data firm that might be a key Trump-Russia link, explained. *Vox*. Retrieved from: https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie

Ingram, M. (2018). Most Americans say they have lost trust in the media. *Columbia Journalism Review*. Retrieved from: https://www.cjr.org/the_media_today/trust-in-media-down.php

Innerarity, D., and Colomina, C. (2020). Introducción: desinformación y poder, la crisis de los intermediarios. *Revista CIDOB d'Afers Internacionals*, 124 (7-10). https:// doi.org/10.24241/rcai.2020.124.1.7

Jackson, D. (2018). The "Demand Side" of the disinformation crisis. International Forum for Democratic Studies. Retrieved from: https://www.ned.org/issue-brief-the-demand-side-of-the-disinformation-crisis/

Jeangène, J-P., Escorcia, A., Guillaume, M., and Herrera, J. (2018). Information Manipulation: A Challenge for Our Democracies. Report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August.

Kramer, A., Guillory, J., & Hanccock, J. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, (111). 24. https://doi.org/10.1073/pnas.1320040111

Lanier, J. (2018). *Diez razones para destruir las redes sociales*. Madrid: Debate.

Levin, S. (2017, May 1). Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

Livingstone, S. (2018). Tackling the Information Crisis: A Policy Framework for Media System Resilience. L. S. E. Truth, Trust and Technology Commission. London: London School of Economics and Political Science. Retrieved from: http://www.lse.ac.uk/media-and-communications/assets/documents/research/T3-Report-Tackling-the-Information-Crisis.pdf

López-Blanco, C. (2019). Wotan, la sociedad abierta y sus nuevos enemigos. *Letras Libres*. Retrieved from: https://www.letraslibres.com/espana-mexico/revista/wotan-la-sociedad-abierta-y-sus-nuevos-enemigos

Mattis, James N. (2005). Future warfare: the rise of hybrid wars. *Proceedings of the U.S. Naval Institute*, (131). Retrieved from: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

Meleshevich, K., and Schafer, B. (2018). Online information Laundering: The Role of Social Media. *Alliance for Securing Democracy*, Policy Brief. No.2. Retrieved from: https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/

Milosevich, M. (2017). El poder de la influencia rusa: la desinformación. Analysis by the Real Instituto Elcano. Retrieved from: https://www.realinstitutoelcano.org/analisis/el-poder-de-la-influencia-rusa-la-desinformacion/

Ng, N., and Rumer, E. (2019). The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture. *Carnegie Endowment for International Peace*.

Nye, J. (2005). *Soft Power: The Means To Success in World Politics*. Public Affairs.

Paris Call (2019). Paris Call for Trust and Security in Cyberspace. Retrieved from: https://pariscall.international/en/

Perrin, W. (2020). Implementing a duty of care for social media platforms, in Renewing Democracy in the Digital Age. Berggruen Institute. Retrieved from: https://www.berggruen.org/ideas/articles/implementing-a-duty-of-care-for-social-media-platforms/

Persily, N. (2017). The 2016 US Election: Can democracy survive the internet? *Journal of Democracy*, 28 (2), 63-76.

Persily, N. (2019). The Internet's challenge to democracy: Framing the problem and assessing reforms. Kofi Annan Foundation. Retrieved from: https://pacscenter.stanford.edu/publication/the-internets-challenge-to-democracy-framing-the-problem-and-assessing-reforms/

Polyakova, A., Kounalis, M., Klapsis, A., Germania, S., Iacoboni, J., Lasheras, B., and de Pedro, N. (2017). The Kremlin's Trojan Horses: Russian Influence in Greece, Italy and Spain. Atlantic Council Eurasia Center.

Reisinger, H. and Golts, A., (2014). Russia's hybrid warfare. Research Paper, NATO Defense College, 105.

Rosenberger, L. and Howard, P. (2020). Disinformation and the Covid Crisis. Global Progress.

Rutenberg, J. (2017, September 13). RT, Sputnik and Russia's new theory of war. *The New York Times*. Retrieved from: https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html

Sanovich, S. (2017). Computation Propaganda in Russia: The Origins of Digital Misinformation. Computational Propaganda Research Project, Working Paper No. 2017/3.

Shepsle, K., and Weingast, B. (1981). Structure-Induced Equilibrium and Legislative Choice. *Public Choice*, 37(3), 503-519.

SCSI (2018). An assessment of the Internet Research Agency's U.S.-directed activities in 2015-2017 based on platform-provided data. Retrieved from: https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Slides.pdf

Simpson, E., and Conner, A. (2020). "Digital Contact Tracing to Contain the Coronavirus". Center for American Progress. Retrieved from: https://www.americanprogress.org/issues/technology-policy/news/2020/04/22/483521/digital-contact-tracing-contain-coronavirus/

Soros, G. (2018). Remarks delivered at the World Economic Forum. Retrieved from: https://www.georgesoros.com/2018/01/25/remarks-delivered-at-the-world-economic-forum/

Soros, G. (2019). Remarks delivered at the World Economic Forum. Retrieved from: https://www.georgesoros.com/2019/01/24/remarks-delivered-at-the-world-economic-forum-2/

Thornhill, J. (2020, March 16). Facebook and the Fifth Estate must do more to fight misinformation. *The Financial Times* https://www.ft.com/content/f1e8f098-6770-11ea-800d-da70cff6e4d3

US v Elena Aleekseevna Khusyaynova (2018). Criminal Complaint. US District Court, Alexandria, Virginia.

Case 1:18-MJ-464.

Wylie, C. (2019). *Mindf*ck: Cambridge Analytica and the Plot to Break America*. New York: Random.

Yin, L., Roscher, F., Bonneau, N., and Tucker, J. (2018). Your Friendly Neighborhood Troll: The Internet Research's Agency's Use of Local and Fake News in the 2016 US Presidential Campaign. SPaPP Data Report 2018:01. Retrieved from: https://s18798.pcdn.co/smapp/wp-content/uploads/sites/1693/2018/11/SMaPP_Data_Report_2018_01_IRA_Links_1.pdf

Zuboff, S. (2020, January 24). You Are Now Remotely Controlled. *The New York Times*. Retrieved from: https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html

Zuckerberg, M. (2019, March 29). The Internet need new rules: let's start in these four areas. *The Washington Post*. Retrieved from: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html