Legal and criminal prosecution of disinformation in Spain in the context of the European Union

Carlos Espaliú-Berdud

Nota: Este artículo se puede leer en español en:
https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/86844

Recommended citation:

Espaliú-Berdud, Carlos (2022). "Legal and criminal prosecution of disinformation in Spain in the context of the European Union". *Profesional de la información*, v. 31, n. 3, e310322.

https://doi.org/10.3145/epi.2022.may.22

Manuscript received on 20th January 2022Accepted on 18th April 2022

Carlos Espaliú-Berdud
https://orcid.org/0000-0003-4441-6684

Universidad Antonio de Nebrija
Santa Cruz de Marcenado, 27
28027 Madrid, Spain
cespaliu@nebrija.es

Abstract

Disinformation poses a very important and growing risk to our society, either alone or in association with other hybrid threats, which is being addressed at both the international and European Union (EU) as well as national level. Within the EU, a multidisciplinary and cooperative approach has been advocated between all the actors involved, in contrast to the strong regulatory perspective traditionally adopted in the history of European integration within the EU framework. For this reason, together with the inherent limitations imposed by the nature of the right to freedom of expression and information on any possible administrative censorship or criminal punishment, Spain has adopted only one recent regulation (*Decree PCM/1030/2020*) to establish the Spanish procedure to combat disinformation as required by European directive. Moreover, although fake news cannot be prosecuted directly in Spain outside the scope of crimes against the market and consumers, fake news can include very different types of criminal offence depending on the content and the intention with which it is disseminated. We illustrate these possibilities through some recent judicial decisions on this matter and declarations by the Office of the Attorney-General. It remains to be seen whether this soft approach to combating disinformation will be sufficient to combat this new plague on our contemporary society effectively.

Keywords

Disinformation; Fake news; Freedom of expression; Freedom of information; Censorship; Cybersecurity; Online platforms; Traditional media; Legacy media; Soft law norms; Hard law norms.

Funding

This article is a result of the project *Mediatized EU,* (*Mediatized discourses on europeanization and their representations in public perceptions*). European Union's H2020 Research and Innovation Programme, Grant agreement no 101004534. SC6, Transformations, 2020.
https://ror.org/00k4n6c32

1. Introduction

In recent years, cyberattacks on both public and private institutions have multiplied in all countries around the world. In fact, according to data from the *National Cryptological Center* of the *Ministry of Defense*, Spain is subject to three critical or highly dangerous cyberattacks against the public sector or strategic companies per day (*National Cryptological Center*, 2019). The origin and purposes of these attacks are varied, but it is particularly worrying that some of them come from states

> "whose purpose is to weaken and compromise Spain's economic, technological, and political capacity in an increasingly complex, competitive, and globalized world" ["*que tienen entre sus propósitos debilitar y comprometer la capacidad económica, tecnológica y política de España en un mundo cada vez más complejo, competitivo y globalizado*"] (*National Cryptological Center*, 2019, p. 4).

Alongside these cyberattacks of great relevance to national interests, there are frequent attacks on all types of entities or individuals, of lesser importance to global interests but clearly still of great importance to the lives of those individuals or entities.

Parallel to these cyberattacks focused on disrupting the computer systems of those affected, other attacks are occurring more and more frequently, the aim of which is to disrupt public opinion, thereby damaging the democratic functioning of democratic states as well as international organizations. This type of action has been included under the already well-known term of "disinformation" campaigns. More precisely, this term can be defined as

> "[...] the intentional dissemination of non-rigorous information that seeks to undermine public trust, distort the facts, transmit a certain way of perceiving reality, and exploit vulnerabilities with the aim of destabilization" ["*[…] la difusión intencionada de información no rigurosa que busca minar la confianza pública, distorsionar los hechos, transmitir una determinada forma de percibir la realidad y explotar vulnerabilidades con el objetivo de desestabilizar*"] (**Olmo-y-Romero**, 2019, p. 4).

In this regard, note that it is not uncommon to associate disinformation campaigns exclusively with well-known phenomena such as fake news, false news, or hoaxes, although, as seen from the various elements of the proposed definition, various other actions should also be included when talking about "disinformation" campaigns. Among these, without being exhaustive, one can mention the news approach, or the use of technical means to manipulate reality, such as algorithms, automated bot accounts, etc. Thus, for example, the Director of the *NATO Center Stratcom Center of Excellence*, Janis Sarts, in his appearance before the *Parliamentary Commission on National Security* of Spain, gave as an example the fact that, according to data collected by researchers of the center he directed, 85% of the content in Russian on *Twitter* in which the words "NATO," "Latvia," or "Estonia" appear was generated by robots (*Cortes Generales*, 2017, p. 15).

By way of illustration, let us indicate the methodology that some of these more serious disinformation campaigns utilize with the aim of destabilizing the attacked society. First, an identification and analysis of the social and political vulnerabilities of the victim of the attack is carried out. Second, transmedia narratives to be disseminated through various communication channels are developed. Third, a network of individual media outlets is set up. Finally, automated distribution channels are created (*National Cryptological Center*, 2019, pp. 17-19).

In this regard, it should be emphasized that, although such deception techniques have always been used to achieve political or war aims (*National Cryptological Center*, 2019, p. 5), today, owing to the technological revolution that has taken place worldwide, their danger and scope have multiplied, constituting a serious global risk (**Shao** *et al.*, 2018, p. 2). Furthermore, experts point to various factors that are contributing to the proliferation of such disinformation campaigns. First, it is necessary to highlight their high level of effectiveness, due to the current technological possibilities, normally affecting social vulnerabilities that already exist in the attacked society. Like weeds among the wheat, elements of illegitimate disinformation are inserted into legitimate social and political communication channels, which increases their apparent veracity. Second, their recurrence is explained by the difficulty of attributing responsibility for such campaigns and the obstacles to identifying the link between an orchestrated campaign and its resulting influence on changes in public opinion through the attacked entities. Finally, the extent and dangerousness of such disinformation campaigns make it intrinsically difficult for democratic societies to prosecute these hostile actions against our societies from a legal point of view, unlike other behaviors whose offensive nature is clearer, such as armed attacks, terrorist actions, or even attacks on computer systems or hacking. Indeed, it is difficult to counteract disinformation without simultaneously attacking the fundamental principles of democratic states and societies, such as freedom of expression and opinion, which underpin the fundamental individual rights of both citizens and foreigners.

In this way, we understand that determining the legal instruments with which states fight disinformation campaigns is not only of interest from a sociological perspective by allowing us to delve into the features and dimensions of this new social phenomenon but also of great legal and political interest by revealing the democratic maturity and level of respect for the rule of law prevai-

> Within the EU, a multidisciplinary and cooperative approach has been advocated between all the actors involved, in contrast to a strong regulatory perspective

ling in these states. In this regard, our aim herein is to shed light on the means by which Spain has been equipped to confront this type of campaign and its perpetrators, in particular through the instruments of criminal law. To this end, we first present the context of EU law within which Spanish legislation is framed. We then analyze the Spanish legislation adopted to counter these new forms of attack focused on fundamental values of society and the tools that criminal law provides for this. Finally, we present some conclusions.

We follow the methodology of the legal sciences, analyzing primary sources such as international treaties and other legal regulations of the EU and the *Council of Europe*, as well as the ad hoc legal regulations adopted in Spain or the appropriate criminal regulations, together with the jurisprudence of the European and Spanish courts on the subject. At the same time, relying on secondary sources, we highlight the most relevant and recent doctrinal developments in the fight against disinformation in Spain.

2. Background regarding the fight against disinformation in the EU

2.1. Awareness of the problem within the limits inherent to the rule of law

As mentioned in the "Introduction," neither states nor international organizations, let alone the EU, are spared from disinformation campaigns.

In this sense, it has been increasingly recognized by the Member States, and by the EU itself, that they have suffered massive disinformation campaigns, especially in electoral or political contexts, either from internal groups, as in the recent electoral campaigns in Germany (**Delcker**; **Janosch**, 2021), or from third countries, with the specific objective of discrediting and delegitimizing elections (*European Commission*, 2018c). Recently for example, in September 2021, the High Representative of the European Union for Foreign Affairs and Security Policy, Josep Borrell, stated that some Member States had observed malicious computer activities, collectively referred to as Ghostwriter, that endangered integrity and security, and linked them to the Russian state. High Representative Borrell stated that such malicious computer activities were directed against parliamentarians, government officials, politicians, and members of the EU press and civil society through access to computer systems and personal accounts, and data theft. Borrell concluded that these activities were contrary to the rules of the responsible behavior of states in cyberspace endorsed by all members of the *United Nations* and aimed at undermining the democratic institutions and processes of the Member States of the EU,

> "[…] in particular by enabling disinformation and manipulation of information." (*Council of the European Union*, 2021).

Indeed, as pointed out by the High Representative of the Union, disinformation campaigns are particularly compromising at the EU level by disrupting the free exercise of freedom of information for malicious purposes, which lies very close to the central core of democratic life in the EU and its Member States. In this regard, it should be recalled that the European Court of Human Rights (ECHR) has reiterated in its jurisprudence that

> "freedom of expression, […] constitutes one of the essential foundations of a democratic society and one of the primary conditions for its progress." (*ECHR*, 1992, *Castells v. España*, para. 42).

Indeed, this reality is inscribed in the fundamental rules of the Union. Thus, article 2 of the *Treaty on European Union* (*TEU*) states that democracy is one of the fundamental values of the UE, and is based on the existence of free and independent media, whose operation requires the full exercise of freedom of expression and information. This freedom is guaranteed, in turn, by article 11 of the *Charter of Fundamental Rights of the European Union*. It should be remembered that, according to this provision, freedom of expression and information includes freedom of opinion, freedom to receive or communicate information or ideas without interference by public authorities and regardless of borders, as well as freedom of the media and its pluralism. Article 10 of the *European Convention on Human Rights* (*ECHR*), which is also part of EU law, recognizes the right to freedom of expression. According to its provisions,

> "This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

However, the provision's text also clarifies that

> "1. […] This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Meanwhile, European jurisprudence, from both the *Court of Justice of the European Union* (*CJEU*) and the *ECHR*, when interpreting and applying this right, has reiterated that any limitation of freedom of expression must be interpreted restrictively and any limitation must be imposed by regulatory provisions (*CJEU*, 2001, *Connolly v European Commission*, para. 42). Of particular interest to our work is the fact that the *CJEU* has warned authorities that they cannot silence opinions, even if they are contrary to the official view (*CJEU*, 2001, *Connolly v. European Commission*, para. 43). Even for the *ECHR*, article 10 of the *ECHR*

> "[…] does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful. To suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media and would thus place an unreasonable restriction on the freedom of expression set forth in Article 10 of the *Convention*." (*ECHR*, 2005, *Salov v. Ukraine*, para. 103).

2.2. Adoption of measures by the EU to combat disinformation

In this context of growing concern about disinformation and the need for the EU to address it, in March 2015, the *European Council* requested that the High Representative of the European Union for Foreign Affairs and Security Policy prepare an action plan on strategic communication (*European Council*, 2015, point 13), which led to the establishment of the *East StratCom Task Force*, operational since September 2015 and part of the *Information Analysis and Strategic Communications Division* of the *European External Action Service*. Its main mission is to develop communication elements and information campaigns aimed at better explaining EU policies in the countries of Eastern Europe.

A few months later, in June 2017, the *European Parliament* began to reflect on the need to adopt legal instruments regarding disinformation and the spread of false content (*European Parliament*, 2017).

In this regard, before getting into our study of the measures adopted by the EU in recent years focused on disinformation, we must point out the need to take into account that this phenomenon can only be addressed from a multidisciplinary perspective, since it affects a multitude of aspects, such as hybrid threats, the digital single market, the regulation of the media in the EU and its Member States, etc. There is no doubt, therefore, that the regulation of the disinformation phenomenon is based on a broad and complex EU regulatory framework, generally from before the explosion of this phenomenon in recent years (**Seijas**, 2020, p. 3). Thus, among many other community regulations involved in a more or less indirect way, one can cite

- *Directive 2013/40/EU*, aimed at the harmonization of the criminal law rules of the Member States in the field of attacks against information systems by establishing minimum rules relating to the definition of criminal offences and applicable sanctions, and improving cooperation between the responsible authorities, including the police and other specialized services;
- *EU Directive 2016/1148*, regarding measures to ensure a high common level of network and information system security in the EU; or
- the package of measures adopted by the *European Commission* in 2018 to ensure free and fair European elections (*European Commission*, 2018c);
- *Directive (EU) 2018/1808* of the *European Parliament and of the Council* of 14 November 2018, which amended *Directive 2010/13/EU* regarding the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services (the *Audiovisual Media Services Directive*), in the light of changing market realities.

Returning to the study of measures taken specifically to tackle disinformation, it is worth highlighting that, in January 2018, the *European Commission* established a high-level group of experts to advise on political initiatives aimed at countering fake news and disinformation disseminated online, which was of great importance for the evolution of EU action in this field. Its final report, published on March 12, 2018, reviews best practices in the light of fundamental principles and appropriate responses derived from those principles, proposing to the *European Commission* a multidimensional approach to this issue (**Renda**, 2018, p. 21), seeking to involve all relevant parties in any future action and insisting on the need for self-regulation. The report also recommended a number of other measures, such as promoting media literacy among the population, developing tools to empower users and journalists to tackle the phenomenon of disinformation, or protecting the diversity and sustainability of European media. As measures aimed in particular at private actors, the report of the expert group advocated the development of a code of principles that online platforms and social networks should endorse, including, for example, the need to ensure transparency when explaining how their algorithms select the news presented. With regard to monitoring the implementation of the proposed measures, the report suggested the establishment of a multilateral coalition of relevant parties to ensure that any measures agreed are implemented, monitored, and regularly reviewed (*European Commission*, 2018, a). It is interesting to note the complete absence of any recommendation to the community bodies regarding the adoption of mandatory legal standards for the Member States (**Jiménez-Cruz** *et al*., 2018).

In response to these suggestions, in March 2018, the *European Commission* and the High Representative of the European Union for Foreign Affairs and Security Policy developed the Action Plan against Disinformation, which was approved by the *European Council* in December 2018 (*European Commission* and *High Representative of the European Union for Foreign Affairs and Security Policy*, 2018). This action plan builds on the recognition of the need for political determination and unified action between EU institutions, Member States, civil society, and the private sector, especially online platforms. This unified action should be based on four pillars:

i) improving the capacities of EU institutions to detect, analyze, and expose disinformation;

ii) strengthening coordinated and joint responses to disinformation;

iii) mobilizing the private sector to tackle disinformation, and

iv) raising awareness and enhancing societal resilience. In this sense, it should be noted that, as stated by Fonseca-Morillo in the conception of the plan,

> "[...] media literacy goes beyond the knowledge of information technologies: it is about developing the critical thinking skills necessary to analyze complex realities and distinguish facts from opinions or create content responsibly" ["*[...] la alfabetización mediática va más allá del conocimiento de las tecnologías de la información: se trata de desarrollar las habilidades de pensamiento crítico necesarias para analizar realidades complejas y distinguir hechos de opiniones o crear contenido de manera responsable*"] (**Fonseca Morillo**, 2020, p. 2).

In the action plan, with regard to the necessary legislative development, the *Commission* and the High Representative requested that Member States implement the provisions contained in Article 33a of *Directive (EU) 2018/1808* on audiovisual media services as soon as possible, which required Member States to promote and take measures for the development of media literacy skills and to report regularly to the *European Commission* on the introduction and implementation of such measures.

As a result of the implementation of the 2018 action plan, the EU's Rapid Alert System was launched, being set up between EU institutions and Member States to facilitate the exchange of information on, and coordinate responses to, disinformation campaigns. The Rapid Alert System is based on open-source information and also draws on the expertise of academia, fact checkers, online platforms, and international partners.

Along the same lines, in April 2018, the *European Commission*, to involve private actors (especially online platforms) in the fight against disinformation, proposed a code of practice (*European Commission*, 2018b) that implies self-regulatory rules that must be voluntarily accepted by private operators to achieve the objectives set by the *European Commission*. These self-regulatory rules set out a wide range of commitments, from transparency in political publicity to the closure of false accounts and the demonetization of disinformation providers. The code of practice was subsequently opened for signature by the main operators in this field, many of which (*Facebook*, *Google*, *Microsoft*, *Mozilla*, *TikTok*, and *Twitter*) had already signed by the mid-2020s (*European Commission*, 2021).

On the other hand, we must remember that the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) pandemic, more popularly known as coronavirus disease 2019 (Covid-19), has been accompanied by powerful disinformation campaigns, further overshadowing the aforementioned panorama, eventually leading the *World Health Organization* (2019, p. 34) to label the situation as an "infodemic."

> "Freedom of expression, which is key to democracy, prevents the imposition of any kind of censorship in the media, even if its content is false. However, the imposition of limits on disinformation is permitted for security or other fundamental reasons"

For example, in a joint communication in June 2020, the *European Commission* and the High Representative of the EU warned that, among the multiple harmful elements of the pandemic, some foreign actors and certain third countries, in particular Russia and China, had undertaken disinformation campaigns concerning Covid-19 in the EU, its surroundings, and on a global scale to undermine the democratic debate and exacerbate social polarization (*European Commission* and *High Representative of the European Union for Foreign Affairs and Security Policy*, 2020, p. 4). In that press release, the *Commission* and the High Representative recommended continuing to act through the instruments available to the EU, building on the December 2018 *Action Plan against Disinformation* and in collaboration with the competent authorities of the Member States, civil society, and social media platforms, with the aim of increasing the resilience of citizens. At the same time, the *Commission* and the High Representative stressed the need for this fight against disinformation to be carried out without undermining freedom of expression and other fundamental rights, as well as democratic values. It should be noted that the *Commission* and the High Representative warned that the Covid-19 crisis had exposed the risk that some measures designed to tackle the "infodemic" would be used as a pretext to undermine fundamental rights and freedoms, or would be abused for political purposes inside and outside the EU. The press release went so far as to point out some deviations from the delicate balance between freedom of expression and the criminal repression of disinformation by Member States. For example, the introduction of a new specific offence of dissemination of disinformation into the Hungarian penal code was seen during the state of alert (*European Commission* and *High Representative of the European Union for Foreign Affairs and Security Policy*, 2020, p. 12-13).

Finally, in December 2020, an Action Plan for European Democracy was adopted, emphasizing the well-known approaches to disinformation and reaffirming that the EU, to preserve and strengthen its democratic life, needs to make more systematic use of the full range of tools it possesses to counter foreign interference and influence operations. There is also an emphasis on the need to further develop these tools, in particular by imposing sanctions on those responsible (*European Commission*, 2020b, p. 24). In relation to the cooperation of online platforms and the usefulness of the Code of Practice on Disinformation, the *Commission* recognized that there was a need for

> "[…] a stronger approach, based on clear commitments and subject to appropriate monitoring mechanisms, to combat disinformation more effectively." (*European Commission*, 2020b, p. 26).

In this regard, the *European Commission* announced that the future Digital Services Act will propose

> "[...] rules to ensure that platforms have greater responsibility when it comes to reporting on how they moderate their content, advertising, and algorithmic processes." (*European Commission*, 2020b, p. 26).

We have referred to the array of measures that the EU has taken in recent years against disinformation, although it is striking that there are no legal acts, such as directives or regulations, from the Member States that are focused on this problem. Undoubtedly, this lack of adoption of hard law norms is due to the sensitivity of this topic, as it is strongly related to freedom of expression and information. This absence was recommended, for example, by the 2018 report from the high-level expert group on disinformation. However, note that, if such disinformation campaigns are part of a hybrid threat from abroad, the primary responsibility for legislating on this matter would rest with the Member States of the EU, since it should not be forgotten that the fight against disinformation campaigns is, to a large extent, a question to be addressed by individual nations. This was highlighted by the *European Commission* and the High Representative of the Union for Foreign Affairs and Security Policy in their 2017 Joint Report to the *European Parliament* and the *European Council* on the implementation of the Joint Communication on Countering Hybrid Threats of April 2016. In the words of those senior European authorities, while the EU can help Member States strengthen their resilience to hybrid threats,

> "[…] the primary responsibility lies with the Member States, as the fight against hybrid threats is a matter of defense and national security." (*European Commission* and *High Representative of the European Union for Foreign Affairs and Security Policy* (2017), p. 2).

For these various reasons, there are no solid EU rules on this subject, and this lack of legal reach, with its consequent negative impact on effectiveness, has already been highlighted by the *European Commission*'s first evaluation report on the implementation and effectiveness of the Code of Practice on Disinformation in 2020 (*European Commission*, 2020a) and has also been strongly criticized by some authors, such as Pamment, for whom the EU's policy on disinformation is characterized:

> "[...] by a lack of terminological clarity, unclear and untested legal foundations, a weak evidence base, an unreliable political mandate, and a variety of instruments that have developed in an organic rather than a systematic manner. The limited successes the EU has achieved so far –in terms of the creation of instruments such as the Code of practice on Disinformation, the Action Plan Against Disinformation, the *East StratCom Task Force*, and the Rapid Alert System– have been hard earned" (**Pamment**, 2020, p. 5).

3. Legal and criminal context of the fight against disinformation in Spain

3.1. Adopting a multidisciplinary lens to link disinformation to cybersecurity instead of adopting specific regulations against it

Spain was established as a democratic society in 1978 and is a member of European international organizations, such as the *Council of Europe* and the EU, which require respect for the rule of law to join them. Spain is thus not oblivious to the legal requirements linked to the impossibility of limiting fundamental rights, such as freedom of expression and information. Therefore, the *Spanish Constitutional Court* (*CC*) has made declarations similar to the European high courts, pointing out, for example, that the rights guaranteed by article 20.1 of the *Constitution* (freedom of expression and information**;** right to literary, artistic, scientific, and technical production and creation; and **freedom to teach)**

> **"[...] are not only an** expression of a basic individual freedom but are also configured as elements shaping our democratic political system" ["*[…] no son sólo expresión de una libertad individual básica sino que se configuran también como elementos conformadores de nuestro sistema político democrático*"] (*Constitutional Court*, 2007, Judgment 235/2007, Legal basis, 4).

On the other hand and in the same way, when freedom of information has come into conflict with other fundamental rights, such as the right to dignity or to one's own image, the *Constitutional Court* has highlighted the prevalent or preferential nature of the freedom of information regarding its reporting capacity of a free public opinion, an essential element of political pluralism in democratic states (*Congreso de los Diputados*, *Spanish Constitution*, synopsis of article 20).

The limitations imposed by the nature of the rights that accompany freedom of expression in the media and on social networks, and the recommendations from the legal instruments and reports from community sources described above, based on a self-regulatory approach encompassing all the actors involved without giving exclusive prominence to the community or national authorities, highlight the fact that there is no criminal law that directly combats disinformation in Spain. Indeed, this problem is being addressed from a multidisciplinary perspective and by linking disinformation to cybersecurity.

In this vein, a national strategy was developed in 2013 and renewed in 2019 and 2021, integrating cybersecurity into the national security system. This strategy is committed to strengthening a strong but perhaps overly complex institutional structure (including the *National Security Council*, *National Cybersecurity Council*, *Situation Committee*, *Standing*

Committee on Cybersecurity, and *National Cybersecurity Forum*), including public–private cooperation, integration into international initiatives, and the development of a culture of cybersecurity, in particular by promoting a critical spirit for the benefit of truthful and high-quality information that contributes to the identification of fake news and misinformation. Thus, it is obvious that, in the context of cybersecurity, regarding the protection of information systems, more specific legal instruments have been adopted in Spain than those intended to protect against disinformation. Among these is *Royal decree 12/2018*, from September 7, concerning the security of networks and information systems, which transfers into Spanish law the *Directive (EU) 2016/1148* outlined above, on measures aimed at ensuring a high common level of security of networks and information systems in the EU. In this regard, it is important to bring up the opinion of the Operating Director of the *Department of National Security*, for whom all these approaches and measures are proving useful, and Spain is in a prominent position, at both a European and global level, in relation to the protection of cybersecurity (*Cortes Generales*, 2019a, p. 12).

> For the time being, Spain has adopted only one recent regulation (*Decree PCM/1030/2020*) to establish the Spanish procedure to combat disinformation as required by European directive. To date, although this law is being challenged in court and in the European Parliament, it has not been declared unlawful

On the other hand, it should be noted that the Government of Spain approved, on November 30, 2021, the draft of the *General Law on Audiovisual Communication* that transfers the audiovisual media services directive reformed in 2018 into the Spanish legal system, and that is currently reaching the end of its parliamentary process. This bill, which falls into the area of protection against disinformation, emphasizes the desirability of adopting voluntary codes of conduct developed by audiovisual media service providers, industry, business, or professional or user associations and organizations (Article 34). Likewise, it insists, in line with regulations adopted in the EU and Spain, on the implementation of measures aimed at the acquisition and development of media literacy skills in all sectors of society (Article 10) (*Congreso de los Diputados*, 2021).

To end this section and illustrate the launch of campaigns in Spain specifically in the field of digital literacy, involving private actors and civil society, we provide Gallardo-Camacho and Marta-Lazo as an example. They point to the initiative of the Atresmedia group, which has opted to implement mechanisms to guarantee the credibility of the news and press services of its two major networks, Antena 3 Noticias and la Sexta Noticias, as well as the opening of online sites to help citizens check the veracity of the content in the press (**Gallardo-Camacho**; **Marta-Lazo**, 2020, p. 5).

3.2. Options for indirect criminal prosecution of conduct involving disinformation in Spain

As noted above, in Spain, the dissemination of false information or fake news, either alone or as possible elements of disinformation campaigns, does not constitute criminal conduct according to the *Criminal Code*. Although this issue has been the subject of strong debate in recent months considering the amount of fake news generated regarding the pandemic, criminalizing these behaviors in and of themselves would go against the fundamental right of freedom of expression established in article 20 of the *Spanish Constitution* of 1978, which we reproduce herein almost entirely because of its centrality in terms of disinformation:

> "Article 20. 1. The following rights are recognized and protected: a) To freely express and disseminate thoughts, ideas, and opinions through speech, writing, or any other means of reproduction. b) Literary, artistic, scientific, and technical production and creation. [...] d) Free communication or receipt of accurate information by any means of dissemination. […]. 2. The exercise of these rights cannot be restricted by any type of prior censorship. […] 4. These freedoms have their limits in respect to the rights recognized in this section, in the precepts of the laws that implement it, and especially, in the right to dignity, privacy, self-image, and protection of adolescence and childhood. 5. The seizure of publications, recordings, and other means of information may be agreed upon only by court order."
>
> ["*Artículo 20. 1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. […] d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. […]. 2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa. […] 4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. 5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial*".]

Thus, with a few exceptions, in the Spanish legal system, disinformation campaigns can only be prosecuted indirectly, on the basis of the consequences of the actions of such campaigns on other, protected legal assets, notwithstanding whether such information or statements have been spread via traditional or online channels. In this latter regard, we point out incidentally that, as Professor Pere Simón warned, the criminal response to opinions spread in the online context does not require the invention of specific responses for this medium by the legislator, but rather the application of

the principles operating in the analogue world, adapted where necessary (**Simón-Castellano**, 2021, p. 189). However, some authors have noticed differences in the judicial treatment of disinformation depending on the channel where it appears. Thus, as Professor Cabellos Espiérrez has shown, the great capacity for content dissemination that is intrinsic to the internet and social networks entails that, in jurisprudential practice in Spain, the criminal treatment of content appearing in such channels,

> "[...]is done in a way that tends to restrict the effectiveness of freedom of expression [...]" ["*[…]se haga de un modo que tiende a restringir la efectividad de la libertad de expresión […]*"] (**Cabellos Espiérrez**, 2018, p. 47).

One of these specific exceptions in which the use of fake news is directly pursued can be understood in a broad sense as evidenced by a report from the Technical Secretariat of the *Office of the Attorney-General* entitled "Criminal treatment of fake news" (*Office of the Attorney-General*, 2020, p. 1), which is constituted by false information in the field of crimes against the market and consumers. Indeed, article 282 of the Criminal *Code* punishes

> "[...] manufacturers or traders who, in their offers or advertising of products or services, make false allegations or manifest uncertain characteristics about them, so that they can cause serious and manifest harm to consumers, without prejudice to the penalty that must be applied for the commission of other crimes" ["*[…] a los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos*"].

Likewise, article 284.1.2 of the *Criminal Code* punishes with imprisonment or a fine those who, by any means, for profit, disseminate false or misleading news or rumors about persons or companies, on the basis of false data.

As mentioned above, apart from these cases, which would not even properly fall within the framework of disinformation described in the beginning, fake news, which is more related to political motivations, can include very different crimes depending on the content and the intention with which it is disseminated. In this work, the presentation of the possible crimes follows the classification proposed in the cited "Criminal treatment of fake news" report from the Technical Secretariat of the *Office of the Attorney-General*.

Thus, fake news can constitute hate crimes under article 510 of the *Criminal Code*, which punishes

> "[...] the expression of epithets, qualifiers, or expressions that contain a message of hatred that is transmitted in a generic way [...]" ["*[…] la expresión de epítetos, calificativos, o expresiones, que contienen un mensaje de odio que se transmite de forma genérica* […]"] (*Supreme Court*, 2018, Fundamento de Derecho Único),

and is likely to generate a climate of hatred, discrimination, hostility, or violence against certain groups. In this regard, paragraph 3 of that article of the *Criminal Code* provides that:

> "The penalties provided for in the preceding paragraphs will be imposed in the upper half of the range when the acts have been carried out through a social communication medium, through the internet, or through the use of information technologies, so that it becomes accessible to a large number of people." ["*Las penas previstas en los apartados anteriores se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas*".]

Recently, in fact, the *Supreme Court* sentenced a person on appeal for a hate crime for issuing expressions inciting hate against a collective on the social network *Twitter* in 2015 and 2016, specifically applying the aggravating circumstance of article 510.3 of the *Criminal Code*, since the author had two accounts on that social network that had around 2,000 followers (*Supreme Court*, 2018, Fundamento de Derecho Único).

In the case where the use of fake news or other possible forms of disinformation is accompanied by the disclosure of real personal data, the *Office of the Attorney-General* considers that such conduct may constitute a crime of discovery and disclosure of secrets described in article 197 of the *Criminal Code* (*Office of the Attorney-General*, 2020, p. 2). Note that the drafting of this article of the *Criminal Code* is the result of the transfer into Spanish law of *Directive 2013/40/EU* on attacks against information systems, which seeks to harmonize the criminal laws of the Member States to curb the

> "[...] threat posed to the EU by the risk of computer attacks of a terrorist or political nature against the computer systems of the Member States' critical infrastructures or of those of the institutions of the EU, and also to the growing trend toward large-scale attacks based on new methods of action, such as the creation and use of infected networks of computers (botnets)" ["*[…] amenaza que supone para la Unión el riesgo de ataques informáticos de carácter terrorista o de naturaleza política contra los sistemas informáticos de las infraestructuras críticas de los Estados Miembros o de las Instituciones de la Unión, e igualmente a la tendencia creciente hacia ataques a gran escala a partir de nuevos métodos de actuación como la creación y utilización de redes infectadas de ordenadores (botnets)*"] (*Office of the Attorney-General*, 2017, p. 2)

Likewise, in the case of fake news that may significantly affect an individual, the crime against moral integrity in article 173.1 of the *Criminal Code* could apply (*Office of the Attorney-General*, 2020, p. 2). In this regard, we must point out how, in the appeal against one of the trials arising from the actions carried out by the notorious "*manada*" in Spain, the defendant's

argument that he had created a website under the name "tourlaManada.com" to denounce the frequent disinformation campaigns that appear in the media was not admitted as a reason for acquittal from the commission of the crime against moral integrity in article 173 of the *Criminal Code*. In fact, for the defendant, the website had not been created to offer a guided tour of the places that the five members of the group visited before the acts constituting the crime of sexual abuse,

> "[...] but a vindictive act to draw attention to the disinformation of the media and its tendency to collect harsh news without verifying sources" ["*[…] sino un acto reivindicativo para llamar la atención sobre la desinformación de los medios y su tendencia a recoger noticias escabrosas sin contrastar fuentes*"] (*Provincial Court of Navarre*, 2020, pp. 4-5). .

Disinformation campaigns or the use of fake news may also include some element of terrorist offences. Thus, on occasion, the perpetrator of a disinformation campaign has been convicted of a terrorist recruitment and indoctrination offense. This was the case, for example, of a self-styled Islamic State militant residing in Melilla who resorted to a disinformation campaign by introducing fake news on Facebook about the conquest of Mosul by the Daesh, and who, in the end, was sentenced in the *National Court* in 2021 for the crime of recruitment and terrorist indoctrination, provided for and punished in article 577.1 and 2 of the *Criminal Code* (*Audiencia Nacional*, 2021, p. 6)

On the other hand, fake news or disinformation campaigns can also be considered to represent acts that violate the right to dignity. Thus, for example, the recent publication on social networks of certain videos concerning a person of public relevance, edited in a biased way, was considered by a judge as a distortion of the original publication's true content as a whole, thus representing a manipulation of public opinion and, therefore, a qualified action of disinformation and intentional manipulation. It should be added that this was one of the elements that led to the conviction of the defendant in the case for violation of the plaintiff's right to dignity (*Provincial Court of Granada*, 2020, Fundamentos de Derecho Primero). Likewise, the *Office of the Attorney-General* believes that fake news can extend to the crimes of slander, from articles 205-206 of the *Criminal Code*, or of defamation, from articles 20–209 of the *Criminal Code* (*Office of the Attorney-General*, 2020, pp. 2–3).

Similarly, fake news regarding possible curative methods without medical confirmation or that are clearly ineffective could constitute one of the crimes against public health provided for in articles 359 et seq. of the *Criminal Code*. However, if these behaviors additionally imply an intention to do business, they would represent a crime of fraud from articles 248 et seq. of the *Criminal Code* (*Office of the Attorney-General*, 2020, p. 3).

3.3. Recent attempts to combat disinformation more directly

After this succinct review of the current state of affairs regarding the possible criminal prosecution of disinformation indirectly through the damage it can do to various legal assets, we must now address the various recent attempts to regulate this issue directly, given the pressing nature of this problem in our society in recent years. In this regard, it should be borne in mind that countries in close proximity to Spain have shown the same concern, particularly in electoral matters. For example, Germany enacted a specific law in June 2017 against posting hate speech, child pornography, terrorism-related articles, and false information on social media, given the inadequacy of voluntary measures taken by social media platforms (*Bundesrepublik Deutschland*, 2017). Likewise, in November 2018, France adopted a law against the manipulation of information, with the objective of better protecting democracy against various forms of intentional dissemination of false news (*République Française*, 2018).

In Spain, it must be noted that, in December 2017, the *Partido Popular* parliamentary group presented a proposal in the *Congress of Deputies* aimed at directly regulating fake news (*Congreso de los Diputados*, 2018). However, this proposal was rejected in March 2018 and was not acted upon (*Cortes Generales*, 2018, p. 5). In addition, in those months, some groups also opposed the regulation of fake news because they understood that such regulation could go against the fundamental right to freedom of expression and was unnecessary because there was already regulation of fake news and propaganda in the *Electoral Law* as well as the *Criminal Code* (*Cortes Generales*, 2019 b).

A few months later, in October 2020, and in the midst of the pandemic, the coalition government formed by the *Spanish Socialist Workers' Party* and *Unidas Podemos* adopted a law to combat disinformation. According to its own text, the purpose of the law is no other than to respond to the requirements of the EU and

> "[...] implement at the national level the policies and strategies promulgated in the field of the fight against disinformation[...]" ["*[...]implementar a nivel nacional las políticas y estrategias promulgadas en el ámbito de la lucha contra la desinformación[...]*"]

and define the bodies, agencies, and authorities that make up the system, as well as define the procedure of their actions (*Government of Spain*, 2020, *Law PCM/1030/2020*). Specifically, within the *National Security System*, an institutional framework was established for the fight against disinformation, consisting of (1) the *National Security Council*, (2) the *Situation Committee*, (3) the *Secretary of State for Communication*, (4) the *Permanent Committee against Disinformation*, (5) the responsible public authorities, and (6) the private sector and civil society. As part of the planned procedure, the law established a series of action or activation levels from the *National Security System* aimed at combating disinformation in view of the danger level of the threat. It should be highlighted that a level 4 is envisaged, which will involve coordination

> "[...] of the response at the political level by the *National Security Council* in case of public attribution of a disinformation campaign to a third State" ["*[…] de la respuesta a nivel político por parte del Consejo de Seguridad Nacional en caso de atribución pública de una campaña de desinformación a un tercer Estado*"] (*Government of Spain*, 2020, *Law PCM/1030/2020*).

In this regard, it is worth highlighting how the doctrine usually warns of the risks and dangers of leaving controlling and limiting powers in matters related to freedom of expression to the administrative authorities, while advancing the desirability of attributing these powers to the judiciary (**Cabellos-Espiérrez**, 2018, p. 48). In fact, the aforementioned 2020 law to combat disinformation was subject to an appeal before the *Supreme Court* by various institutions and for various reasons, but in particular because its implementation would imply a kind of prior censorship, likely to jeopardize the right to freedom of expression and the right to information, without the due guarantees required by the *Spanish Constitution* for the limitation of fundamental rights, or for not respecting the organic structure provided for in *Law 36/2015 on National Security*. The *Supreme Court* has issued decisions on incidental or procedural legitimacy matters regarding the plaintiffs (*Supreme Court*, 2021a; b; c; d), but in a recent judgment, from October 18, 2021, it entered the main substance of the matter. In it, the *Supreme Court* rejected the basis of the contentious administrative appeal filed by *Confilegal*, which, in essence, attacked the provisions of *Law PCM/1030/2020* because it gave prominence regarding actions to be taken against disinformation to the *Department of National Security*, whose action lies beyond judicial control, thus depriving the *National Intelligence Center* of its primary role and

> "[...] which is deprived of the functions attributed by article 4 of Law 11/2002, functions that it performs – and here would be the core of its challenge – under judicial control [...]" ["*[…] que queda desapoderado de las funciones atribuidas por el artículo 4 de la Ley 11/2002, funciones que desempeña – y aquí estaría el meollo de su impugnación – bajo control judicial[…]*"] (*Supreme Court*, 2021, and *Fundamento de Derecho Sexto*).

However, for the *Supreme Court*, the contested law fully respects the organic and jurisdictional structure provided for in *Law 36/2015 regarding National Security* and, therefore, it declared the law to be in accordance with the legal structure (*Supreme Court*, 2021e, Ruling).

A question regarding *Law PCM/1030/2020* was also addressed to the *Commission* in the *European Parliament* in November 2020. In particular, the *Commission* was first asked whether it had analyzed the fact that the monitoring committee proposed in the law under examination

> "[…] is controlled by the Secretary of State for Communication, which reports directly to the *Ministry of the Presidency*, and that the order speaks of examining 'the freedom and pluralism of the media'?" ["*[...] está controlado por la Secretaría de Estado de Comunicación, que depende directamente del Ministerio de la Presidencia, y de que la orden habla de examinar 'la libertad y pluralismo de los medios'?*"].

Additionally, the *Commission* was asked whether it considered

> "[…] that the content of the government decision is irrelevant and that it is sufficient to use the pretext of the fight against disinformation to accept any measure" ["*[…] que el contenido de la decisión gubernamental no tiene relevancia y que es suficiente con utilizar el pretexto de la lucha contra la desinformación para aceptar cualquier medida*"] (*European Parliament*, 2020).

And on February 25, 2021, Vice President Jourová, on behalf of the *Commission*, responded in writing noting that the Ministerial Order in question

> "[...] updates the existing Spanish system to prevent, detect, and respond to disinformation campaigns and to establish coordination structures" ["*[…] actualiza el sistema español existente para prevenir, detectar y responder a las campañas de desinformación y para establecer estructuras de coordinación*"] [...], and "[...] it does not constitute a legal basis for deciding on the content of information provided by the media" ["*[…] no constituye una base jurídica para decidir sobre el contenido de la información facilitada por los medios de comunicación*"].

In addition, in the *Commission*'s view,

> "[...] the Permanent Committee is responsible for monitoring and evaluating online disinformation campaigns, investigating their origin, and determining whether the case should be referred to the *National Security Council* for a political response, such as diplomatic action or retaliatory measures when the perpetrator is a foreign state. This work is the responsibility of the central government and is in line with the 2018 Action Plan against Disinformation, which called on Member States to strengthen their capacities in the fight against disinformation." (*European Parliament*, 2021).

4. Conclusions

In this paper, we have analyzed the different legal ways to prosecute disinformation in Spain, which were already provided for by criminal law, and the attempts made in recent years (when the phenomenon reached very worrying dimensions) to legislate and control it through other channels. We have contextualized this legal study in the fight against disinformation within the EU, to determine, where appropriate, the possible origin, context, and motivation of Spanish regulations.

This research thereby highlights the important limit that every democratic entity encounters concerning the right to freedom of expression and information when it comes to fighting disinformation. We must emphasize that this freedom has been recognized as fundamental and inherent to the rule of law, in both the legal regulation and Spanish communities, by the most relevant European and national instruments in the field, such as the *TEU*, the *Charter of Fundamental Rights of the European Union*, the *ECHR*, or the *Spanish Constitution*, as well as by the consolidated jurisprudence of European and national courts. Thus, freedom of expression goes so far as to allow criticism of community or national authorities, whether spread through traditional media or new social networks, even if not true. Any limitation to this, which must be based on assessed national security or other legitimate grounds, must be imposed by law, as well as subject to the relevant parliamentary and judicial guarantees. Any type of administrative censorship of content outside these parameters is alien to European values and foreign to the Spanish legal system.

> "It remains to be seen whether this soft approach or the recourse to soft law measures to combat disinformation will be sufficient to defeat this new plague on our contemporary society"

For these reasons, we find that, at the EU level, disinformation has been fought with a series of non-normative measures that advocate a multidisciplinary and cooperative approach among all the actors involved, from EU authorities to online platforms through the Member States. As a corollary, that same approach has been the framework that has been followed in Spain. Thus there is only one recent regulation to fight disinformation in a direct and specific way, *Law PCM/1030/2020*, which rather than regulating content, tries to respond to the European directive requiring the implementation of procedures and organic structures in each Member State to fight disinformation. Although the law in question has been appealed through the courts, mainly on the basis of the fear of the absence of judicial guarantees in the procedure, all judicial decisions have so far declared it to be in accordance with law, as has the *European Commission* when questioned in the European Parliament on the matter.

In this way, although the debate on the adequacy of fighting disinformation through solid legal regulations or hard law remains open (**Magallón-Rosa**, 2019, p. 345), it seems that the field is moving to support cooperation between international and national authorities, self-regulation by private actors, such as online platforms, or launching educational campaigns among the population to increase their resilience to the problem. In this vein, we described herein the specific case of digital literacy promotion by an important audiovisual group in Spain to try to guarantee the veracity of the content offered in its newscasts, and to teach users to identify hoaxes in social networks.

It remains to be seen whether this soft approach, or recourse to soft law measures to combat disinformation, will be sufficient to defeat this new plague on our contemporary society.

It would be highly desirable if the Russian invasion of Ukraine and the fake news accompanying this war could serve as a definitive wake-up call to raise awareness of the importance of these issues.

5. References

5.1. Official, normative and jurisprudential documentary references

Audiencia Nacional (2021). Sala de lo Penal, Sentencia 18/2021, de 6 de octubre.

Audiencia Provincial de Granada (2020). Sentencia 414/2020, de 18 de diciembre.

Audiencia Provincial de Navarra (2020). Sentencia 155/2020, de 3 de junio.

Bundesrepublik Deutschland (2017). "Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)".
https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

Centro Criptológico Nacional, *Ministerio de Defensa* (2019). "Desinformación en el ciberespacio", CCN-CERT, BP/13.
https://www.dsn.gob.es/sites/dsn/files/CCN-CERT_BP_13_Desinformaci%C3%B3n%20en%20el%20Ciberespacio.pdf

Comisión Europea (2018a). "A multi-dimensional approach to disinformation". *Report of the independent High level Group on fake news and online disinformation.*
https://www.ecsite.eu/sites/default/files/amulti-dimensionalapproachtodisinformation-reportoftheindependenthighlevelgrouponfakenewsandonlinedisinformation.pdf

Comisión Europea (2018b). "Código de buenas prácticas de la Unión en materia de desinformación".
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59111

Comisión Europea (2018c). "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. 'Garantizar unas elecciones europeas libres y justas - Contribución de la Comisión Europea a la reunión de dirigentes en Salzburgo' los días 19 y 20 de septiembre de 2018", COM(2018) 637, Bruselas, 12 de septiembre.

Comisión Europea (2020a). "Commissión Staff Working Document. Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, SWD(2020) 180 final", Brussels, 10 September. *https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement*

Comisión Europea (2020b). "Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Sobre el Plan de Acción para la Democracia Europea, COM(2020) 790 final", Bruselas, 3 de diciembre.

Comisión Europea (2021). "Comunicado de Prensa, 1 de octubre de 2021. Código de Buenas Prácticas en materia de Desinformación: la Comisión se congratula de los nuevos signatarios previstos y reclama una revisión firme y oportuna". *https://ec.europa.eu/commission/presscorner/detail/es/IP_21_4945.*eu

Comisión Europea y Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (2016). "Comunicación conjunta al Parlamento Europeo y al Consejo. Comunicación conjunta sobre la lucha contra las amenazas híbridas - Una respuesta de la Unión Europea", JOIN (2016) 18 final, Bruselas, Bruselas, 6 de abril.

Comisión Europea y Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (2017). "Informe conjunto al Parlamento Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas - Una respuesta de la Unión Europea, JOIN(2017) 30 final", Bruselas, 19 de julio.

Comisión Europea y Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (2018). "Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción contra la desinformación, JOIN(2018) 36 final", Bruselas, 12 de diciembre. *https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf*

Comisión Europea y Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (2020). "Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La lucha contra la desinformación acerca de la Covid-19: contrastando los datos, JOIN(2020) 8 final", Bruselas, 10 de junio.

Congreso de los Diputados (2011). "Constitución Española, Sinopsis del artículo 20, Libertades de expresión y de información. Sinopsis realizada por: Elvira Perales, Ascensión (2003). Actualizada por González-Escudero, Ángeles" (2011). *https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=20&tipo=2*

Congreso de los Diputados (2018). "Proposición no de Ley relativa al impulso de las medidas necesarias para garantizar la veracidad de las informaciones que circulan por servicios conectados a Internet y evitar injerencias que pongan en peligro la estabilidad institucional en España (162/000550)". *Boletín Oficial de las Cortes Generales*, Serie D, n. 280, 12 de enero.

Congreso de los Diputados (2021). "Proyecto de Ley General de Comunicación Audiovisual (121/000076)". *Boletín Oficial de las Cortes Generales*, Serie A, n. 77-1, 17 de diciembre.

Consejo de la UE (2021). "Comunicado de prensa, 24 de septiembre de 2021, Declaración del alto representante, en nombre de la Unión Europea, sobre el respeto de los procesos democráticos de la UE". *https://www.consilium.europa.eu/es/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes*

Consejo Europeo (2015). "Conclusiones de la Reunión del 19 y 20 de marzo de 2015, Documento EUCO 11/15 CO EUR 1 CONCL 1". Bruselas, 20 de marzo. *https://www.consilium.europa.eu/media/21872/st00011es15.pdf*

Cortes Generales (2017). Comisión Mixta de Seguridad Nacional. "Comparecencia del Director of the NATO Stratacom Center of Excellence, Señor Sarts, para informar sobre diversas cuestiones relativas a la ciberseguridad en España". [Núm. expte. 219/000926 (CD) y núm. expte. 715/000308 (S)]. Sesión de 14 de diciembre, p. 15.

Cortes Generales (2018). *Boletín Oficial de las Cortes Generales*, Serie D, n. 322 21 de marzo.

Cortes Generales (2019a). "Comparecencia del Director Operativo del Departamento de Seguridad Nacional, señor Castellón Moreno, para informar sobre diversas cuestiones relativas a la ciberseguridad en España, Cortes Generales, Comisión Mixta de Seguridad Nacional, aprobación del Informe de la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España", *Boletín Oficial de las Cortes Generales*, Serie A: Actividades Parlamentarias, 13 de marzo, n. 277.

Cortes Generales (2019b). Comisión Mixta de Seguridad Nacional, "Aprobación del Informe de la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España". *Boletín Oficial de las Cortes Generales*, Serie A: Actividades Parlamentarias, 13 de marzo, n. 277.

Fiscalía General del Estado (2017). "Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos".
https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS-C-2017-00003

Fiscalía General del Estado (2020). Secretaría Técnica. "Tratamiento penal de las "*Fake News*"".
https://www.icab.es/export/sites/icab/.galleries/documents-noticies/tratamiento-penal-de-las-fake-news-fiscalia-general-del-estado.pdf

Gobierno de España (2018). "Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión". *BOE*, n. 218, de 8 de septiembre.

Gobierno de España (2019). Presidencia del Gobierno, "Estrategia Nacional de Ciberseguridad", febrero.

Gobierno de España (2020). "Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional", *BOE* n. 292, de 5 de noviembre.

Organización Mundial de la Salud (2018). World Health Organization, "Managing epidemics: key facts about major deadly diseases".
https://www.who.int/emergencies/diseases/managing-epidemics-interactive.pdf

Parlamento Europeo y Consejo (2013). "Directiva (UE) 2013/40 del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo", *DOUE* L 218/8, de 14 de agosto.

Parlamento Europeo y Consejo (2016). "Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión", *DOUE* L 194, de 19 de julio.

Parlamento Europeo (2017). "Resolución del Parlamento Europeo, de 15 de junio de 2017, sobre las plataformas en línea y el mercado único digital (2016/2276(INI))".
https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_ES.pdf?redirect

Parlamento Europeo (2020). "Preguntas Parlamentarias*,* Pregunta con solicitud de respuesta escrita E-006087/2020 a la Comisión, de 10 de noviembre de 2020, Asunto: Plan del Gobierno de España contra la desinformación".
https://www.europarl.europa.eu/doceo/document/E-9-2020-006087_ES.html

Parlamento Europeo (2021). "Preguntas Parlamentarias*,* Respuesta de la Vicepresidenta Jourová en nombre de la Comisión Europea, de 15 de febrero de 2021. Referencia de la pregunta: E-006087/2020".
https://www.europarl.europa.eu/doceo/document/E-9-2020-006087-ASW_ES.html

République Française (2018). "Loi no 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information".
https://www.legifrance.gouv.fr/download/pdf?id=6-nJtAIQpD8-Ugn4wumM7q3PzXyh2U2x_naRfEud_Wg=

TEDH (1992). Sentencia de 23 de abril, *Castells c. España*.

TEDH (2005). Judgment of 6 September, *Salov v. Ukraine.*

TJUE (2001). Sentencia del Tribunal de Justicia de 6 de marzo, *Bernard Connolly c Comisión Europea*.

Tribunal Constitucional (2007). Sentencia 235/2007, de 7 de noviembre.

Tribunal Supremo (2018). Sala de lo Penal, Sentencia 72/2018, de 09 de febrero.

Tribunal Supremo (2021a). Sala de lo Contencioso-Administrativo, Auto de 4 de enero.

Tribunal Supremo (2021b). Sala de lo Contencioso-Administrativo, Auto de 3 de marzo.

Tribunal Supremo (2021c). Sala de lo Contencioso-Administrativo, Auto de 12 de abril.

Tribunal Supremo (2021d). Sala de lo Contencioso-Administrativo, Auto de 13 de mayo.

Tribunal Supremo (2021e). Sala de lo Contencioso-Administrativo, Sentencia 1238/2021, de 18 de octubre.

5.2. Bibliographic references

Cabellos-Espiérrez, Miguel-Ángel (2018). "Opinar, enaltecer, humillar: respuesta penal e interpretación constitucionalmente adecuada en el tiempo de las redes sociales". *Revista española de derecho constitucional*, n. 112.
https://doi.org/10.18042/cepc/redc.112.02

Delcker, Janosch (2021). "Alemania: desinformación y noticias falsas asedian la campaña electoral". *DW*, 7 septiembre.
https://www.dw.com/es/alemania-desinformaci%C3%B3n-y-noticias-falsas-asedian-la-campa%C3%B1a-electoral/a-59113186

Fonseca-Morillo, Francisco (2020). "Prólogo: La Europa que protege, de la teoría a la práctica gracias al pensamiento crítico y la alfabetización digital". *Revista de estilos de aprendizaje*, v. 13, n. 26, pp. 1-3.
https://doi.org/10.55777/rea.v13i26.2593

Gallardo-Camacho, Jorge; **Marta-Lazo, Carmen** (2020). "La verificación de hechos (fact checking) y el pensamiento crítico para luchar contra las noticias falsas: alfabetización digital como reto comunicativo y educativo". *Revista de estilos de aprendizaje*, v. 13, n. 26, pp. 4-6.
https://doi.org/10.55777/rea.v13i26.2594

Jiménez-Cruz, Clara; **Wardle, Claire**; **Kelis Nielsen, Rasmus**; **Mantzarlis, Alexios** (2018). "Seis puntos claves del informe sobre desinformación del grupo de expertos de la Comisión Europea". *Maldita*, 12 marzo.
https://maldita.es/maldita/20180312/seis-puntos-claves-del-informe-sobre-desinformacion-del-grupo-de-expertos-de-la-comision-europea

Magallón-Rosa, Raúl (2019). "La (no) regulación de la desinformación en la Unión Europea. Una perspectiva comparada". *UNED. Revista de derecho político*, n. 106, pp. 319-347.
https://doi.org/10.5944/rdp.106.2019.26159

Olmo-y-Romero, Julia-Alicia (2019). "Desinformación: concepto y perspectivas". *Real Instituto Elcano*, ARI 41/2019.
http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari41-2019-olmoromero-desinformacion-concepto-y-perspectivas

Pamment, James (2020). "The EU's role in fighting disinformation: Taking back the initiative". *Carnegie Endowment for International Peace*, working paper, June.
https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf

Renda, Andrea (2018). "The legal framework to address 'fake news': possible policy actions at the EU level". *CEPS research report*.
https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf

Seijas, Raquel (2020). "Las soluciones europeas a la desinformación y su riesgo de impacto en los derechos fundamentales". *IDP, Revista de internet, derecho y política*, n. 31.
https://raco.cat/index.php/IDP/article/view/373664/467277

Shao, Chengcheng; **Ciampaglia, Giovanni-Luca**; **Varol, Onur**; **Yang, Kai-Cheng**; **Flammini, Alessandro**; **Menczer, Filippo** (2018). "The spread of low-credibility content by social bots". *Nature communications*, v. 9, 4787.
https://doi.org/10.1038/s41467-018-06930-7

Simón-Castellano, Pere (2021). "Internet, redes sociales y juicios paralelos: un viejo conocido en un nuevo escenario". *Revista de derecho político*, n. 110.
https://doi.org/10.5944/rdp.110.2021.30332