The Impact of Disinformation on the Functioning of the Rule of Law and Democratic Processes in the Eu

Maria Romana Allegri

Prof., Sapienza University of Rome

Received: 25 December 2023 / Accepted: 25 February 2024 / Published: 23 April 2024

Doi: 10.56345/ijrdv11n1s116

Abstract

Disinformation and propaganda are based on the fact that the information: i) is designed to be totally or partially false, manipulated or misleading or uses unethical persuasion techniques; ii) concern a matter of public interest; (iii) is intended to generate insecurity, hostility or polarization or attempt to undermine democratic processes; iv) is disseminated and/or amplified using automatic and aggressive tools, such as social bots, artificial intelligence, micro-targeting or paid human trolls, often with the aim of increasing the public visibility of the content. Especially the systematic dissemination of disinformation by active politicians, parties or authorities is a clear and immediate threat to democracy and is disrespectful of the values of the European Union according to Article 2 TEU, because the trust in such authoritative persons is a value choice which cannot be changed by rational arguments. Moreover, deepfakes (algorithmically generated messages flooding recipients to give a false impression of political consensus) present a significant challenge for democracy, because they may sow uncertainty which may, in turn, reduce trust in news on social media and hinder civic participation in online debates. Finally, a study commissioned by the European External Antion Service, published in 2021, has focused on two more categories of disinformation: 'influence operations' by third countries, aimed at influencing a target audience using a range of illegitimate and deceptive means, and 'foreign interference', aimed at disrupting the free formation and expression of political will. Therefore, among the many issues dealt with by the EP resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, it must be mentioned the fact that foreign interference, including disinformation, is a national and cross-border security threat. Consequently, the EP has stressed the need for solidarity between the Member States so that such activities can be effectively combated, also amending Article 222 TFEU (the solidarity clause) by including foreign interference. In fact, with respect to disinformation a process of securitization is being promoted, consisting of applying security tools and discourses upon an object that was previously not identified as such. An example of this trend is represented by the specific task force set up within the European External Action Service in order to address Russia's ongoing disinformation campaigns. Another example, showing that disinformation has become a CFSP issue, is the Council regulation (EU) 2022/350 of 1 March 2022, based on Council decision (CFSP) 2022/351, concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine. However, when determining the focus and political actions of the EU against disinformation, two opposing logics – securitization and self-regulation – coexist and compete. As a result, the EU is promoting a discourse linking disinformation to security, exceptionality and geopolitical strategies, but being lax at the same time with the obligations and responsibilities of the digital platform companies.

Keywords: *Impact of Disinformation, Rule of Law, Democratic Processes in the Eu*

1. Introduction

War has always been based on disinformation, but the one currently underway in Ukraine is probably the first in which social media have played a significant role, that of acting as a privileged channel for the dissemination of both real-time information on the evolution of the conflict and news that differs from reality and is capable of distorting the reality of the

facts on a global level1. The result is a fairly complex picture, where information activity in the context of armed conflicts can be displayed in different areas and have a multiplicity of effects on the target State and on civil society, depending on the technology used, the level of sophistication of the means employed and of the aim pursued2. The category of disinformation and the related but distinct category of propaganda calls into question an unprecedented interaction between different regulatory sectors, such as the audiovisual one, the criminal one and lastly that relating to the regulation of digital services. Therefore, the actions and tools adopted by the Union to deal with disinformation have been, on the one hand, translated from already existing concepts, such as those relating to illegal content, and on the other hand they have integrated new concepts such as the fight against hybrid threats conducted at the level of external relations3.

Hybrid threats, consisting of a combination of conventional and unconventional, military and non-military activities, including disinformation campaign, were clearly addressed by the EU external action service (EEAS) in the light of the degradation of relations with Russia in the aftermath of the annexation of Crimea in March 20144. The incorporation of the digital dimension in the EU's security policies has gradually thus become the EU's new ambition5. The transformation of disinformation into a security issue is part of a broader process known as "securitization", that happens when a certain issue is designated as an existential threat to certain referent objects, and requires urgent and extraordinary actions, which can be justified due to the need for protection of the referent object6. Such extraordinary and urgent measures often go beyond the regular political rules and procedures, being legitimized by "speech acts" portraying an exceptional threat as a danger for security. Speech act is indeed a key tool to legitimize extraordinary measures which normally would not be accepted by the audience. In fact, the evidence of a securitization process applied to disinformation can be captured in the EU's speeches, documents, and the adoption of numerous policy actions, which constructed the disinformation as a vital threat to the EU's existence. However, it has to be considered that the securitization of disinformation may lead to three negative consequences: firstly, it may undermine the freedom of expression and information; secondly, it may cause censorship in social media; thirdly, it can be used for legitimizing strict legislation and abuse of citizens' rights by some of the European governments.

The purpose of this paper, therefore, is to analyze the development of this process through the documents produced by the EU institutions, also highlighting the risks and inconsistencies related to it.

2. The Complex Notion of Disinformation and its Risks

According to the final report of the high-level Group of experts (HLEG) set up by the EU in 2018 to advise on policy initiatives to counter fake news and disinformation spread online, disinformation consists of «all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit»7. Namely, falsity, intention to strategic manipulation and impact on society are the three distinguishing features of this phenomenon8. More precisely, a distinction needs to be made among misinformation (harmless content, although false or distorted), disinformation (false or distorted contend, intentionally disseminated to cause harm), and malinformation (genuine information intentionally shared to cause harm)9. Therefore, the information shared with malicious intent is recognized as disinformation, whereas the same information shared by a poorly informed party is viewed as misinformation10. It has been noted that «disinformation invites looking at more systematic disruptions of authoritative information flows due to strategic deceptions that may appear very credible to those consuming them»11, because of the breakdown of trust in democratic institutions of press and politics combined with the growth of alternative information channels12. Disinformation in its various manifestations has become a systemic challenge for democracies because of

[1] *Mezzanotte M., 2022, p. 45.*
[2] *Mezzanotte M., 2022, p. 46.*
[3] *Lattanzi S., 2022, p. 163.*
[4] *EEAS, A Europe that Protects: Countering Hybrid Threats, June 2018, https://www.eeas.europa.eu/node/46393_en*
[5] *Fernandes S., 2018, p. 46.*
[6] *The securitization theory has been propelled in the Nineties by three scholars – Barry Buzan, Ole Waever, and Jaap de Wilde – which framed the prominent Copenhagen School of securitization discourse.*
[7] *HLEG, 2018, p. 3.*
[8] *Bayer J. and Others, 2021, p. 36.*
[9] *Wardle C. and Derakhshan H., 2017.*
[10] *Bayer J. and Others, 2019, p. 26.*
[11] *Bennet W. L. and Livingston S., 2018, p. 124.*
[12] *Bennet W. L. and Livingston S., 2018, p. 126 and 128.*

the combination of disruptive technological, political and sociological transformations of the public spheres in a very short period of time13.

Disinformation is often combined with propaganda, that is «the systematic dissemination of information, esp. in a biased or misleading way, in order to promote a particular cause or point of view»14. Propaganda can also be meant as «dissemination of information – facts, arguments, rumors, half-truths, or lies – to influence public opinion» and as «the more or less systematic effort to manipulate other people's beliefs, attitudes, or actions by means of symbols», often conveyed through mass media15. Propaganda may or may not include falsified elements and fake news (disinformation), but in all cases it aims to influence and manipulate an opinion to achieve strategic effects in the interest of the propagandist16.

Both disinformation and propaganda are based on the fact that the information: i) is designed to be totally or partially false, manipulated or misleading or uses unethical persuasion techniques; ii) concern a matter of public interest; (iii) is intended to generate insecurity, hostility or polarization or attempt to undermine democratic processes; iv) is disseminated and/or amplified using automatic and aggressive tools, such as social bots, artificial intelligence, micro-targeting or paid human trolls, often with the aim of increasing the public visibility of the content17. This produces a significant impact on public discourse and on voting behaviour, since participatory and deliberative democracy require the provision of information and effective processes of consultation and the passive side of free speech incorporates the public's right to receive information, in order to allow a conscious participation in public debate.

The challenge posed by disinformation and propaganda comes not only from its content, but also how it is distributed and promoted on social media. In fact, the intention to harm or profit entails that disinformation is commonly accompanied by strategies and techniques to maximise its influence18. False or misleading content is transmitted, organized, and amplified by social media platforms, making extensive use of aggressive dissemination practices, such as micro-targeted political advertising, paid trolls and political bots (algorithmically generated messages designed to persuade targeted audiences or to give a false impression of political consensus). Additionally, social media results allow the constant adaptation of the algorithms, offering an excellent arena in which to study human behaviour and to design tailored manipulative campaigns19. Moreover, deepfakes (deep machine-learning technology used to fabricate realistic audiovisual media) represent a significant challenge for democracy, because they may sow uncertainty which may, in turn, reduce trust in news on social media and hinder civic participation in online debates20. These aggressive practices may be employed to promote false or manipulated content, as well as genuine information or value judgment-like statements that cannot be objectively verified, thus interfering with democracy in two ways: (i) they dominate and distort the public discourse and corrupt the process of democratic decision-making, and (ii) they help successful leaders capture the state and deconstruct the constitutional system21. Notably, if democracy is manipulated by techniques of persuasion that are not compliant with the rule of law and infringe fundamental rights, the procedure itself might be a threat to democracy22. In fact, being the EU a *sui generis* formation of sovereign states, European democracy is rooted in the democratic legitimacy of the representatives of Member States: if concerted disinformation and propaganda campaigns render this legitimacy questionable, then the democratic legitimacy of EU institutions and their actions becomes questionable as well23.

The most systemic threats to political processes and human rights arise from organized attempts to run coordinated campaigns across multiple social media platforms 24 . Such concerted efforts require large financial resources: this is why disinformation campaigns are often effectively organized by government actors or private actors supported implicitly or explicitly by foreign governments – for example Russia's demonstrated influences in the Brexit

[13] *Casero-Ripollés A. and Others, 2023, p. 3.*
[14] *According to the Oxford English Dictionary.*
[15] *B. L. Smith in Encyclopedia Britanica, January 2024.*
[16] *Robin M., 2023, p. 1.*
[17] *Bayer J. and Others, 2019, p. 18.*
[18] *Colomina C. and Others, 2021, p. 5.*
[19] *Bayer J. and Others, 2019, p. 59.*
[20] *Bayer J. and Others, 2021, p. 25. About the dangers related to deepfakes see also Mezzanotte M., 2022.*
[21] *Bayer J. and Others, 2019, p. 11.*
[22] *Bayer J. and Others, 2019, p. 60.*
[23] *Bayer J. and Others, 2019, p. 16.*
[24] *Colomina C. and Others, 2021, p. 6.*

process and in the 2019 European elections by means of the so called "Potemkin personas"25 – who can count on them. Therefore, citizens «are under increasing and systematic pressure to process information, disinformation and misleading information campaigns and propaganda coming from countries and non-state actors, such as transnational terrorist or criminal organizations in its vicinity, which seek to undermine the very notion of objective information or ethical journalism, by disseminating only biased information or information used as a tool for political power, and which also undermine democratic values and interests»26.

Especially the systematic dissemination of disinformation by active politicians, parties or authorities is a clear and immediate threat to democracy and is disrespectful of the values of the European Union according to Article 2 TEU, because the trust in such authoritative persons is a value choice which cannot be changed by rational arguments27. And, notably, systemic violations of the values enshrined in Article 2 TEU may undermine the effectiveness of mutual trust-based instruments and even jeopardize the principle of primacy of EU law28. For all these reasons, following a precautionary logic the protection of democracy today implies the display of robust precautionary measures in democratic systems to make them resilient against future potential authoritarian and illiberal political tendencies29. Nevertheless, while disinformation threatens human rights, the inverse challenge is that counter-disinformation policies can also restrict freedoms and rights. Consequently, in defending measures to tackle disinformation, the European Union must be careful to

tackle both human rights impacts resulting from disinformation and any rights abuses inadvertently caused by attempts to counter disinformation30.

3. Self-Regulative and Co-Regulative Instruments Against Information Disorders

The EU policy on disinformation responds essentially to increasing aggressiveness of Russia and to the effects of the COVID-19 pandemic. In the last years, several European legal and policy instruments have addressed the information ecosystem, and each made mention of disinformation, the most relevant of which being the well-known Code of Practice on Disinformation31, released in 2018 and strengthened in 2022, as well as the European Democracy Action Plan (EDAP)32, adopted in 2020 and renewed in 202333, that defined various types of disinformation, and identified certain strategies to be applied. In particular, it identifies the concepts of "information influence operations" (coordinated efforts to influence a targeted audience by deceptive means) and "foreign interference in the information space" (when such efforts involve a foreign state actor or its agents) 34, both aimed at disrupting the free formation and expression of political will. EDAP has made clear that the fight against disinformation involves various instruments to counter foreign interference, including the possibility of imposing sanctions on those responsible, in accordance with European values and principles. Also, the recent EU regulation on digital services35 (Digital Services Act – DSA) mentions disinformation36 among the systemic risks to be assessed in-depth and possibly prevented or at least mitigated by the providers of very large online platforms and of very large online search engines37. Disinformation is also a crucial issue in the proposal of a European Media Freedom Act38 and that of a regulation on the transparency and targeting of political advertising39, whose definitive adoption by the European Parliament and the Council is expected soon. In fact, the high protection of political speech makes the fight against disinformation particularly complex for democratic societies, especially in sensitive moments such as elections and referendums.

---

[25] According to Bayer J. and Others, 2021, p. 21, Potemkin personas «are foreign, and in this context, typically Russian trolls who build a credible online presence across multiple platforms and mix their political messaging with banal posts about their supposed daily life».
[26] Robin M., 2023, p. 1.
[27] Bayer J. and Others, 2019, p. 111.
[28] Bayer J. and Others, 2019, p. 69.
[29] Bayer J. and Others, 2019, p. 67.
[30] Colomina C. and Others, p. 9 and 16.
[31] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[32] COM(2020) 790 of 3 December 2020: https://commission.europa.eu/document/63918142-7e4c-41ac-b880-6386df1c4f6c_en
[33] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en
[34] Colomina C. and Others, 2021, p. 5.
[35] Regulation (EU) 2022/2065 of 19 October 2022.
[36] Whereas no. 2, 9, 69, 83, 84, 88, 95, 104, 106, 108.
[37] Articles no. 33-36.
[38] COM(2022) 457 of 16 September 2022. See the comment by Cabrera Blázquez F. J., 2022.
[39] COM(2021) 731 of 25 November 2021. See Pollicino O. and De Gregorio G., 2023.

The EU approach combines a narrow set of legal obligation with a wider range of co-regulative and self-regulative measures. To improve the fight against biased or erroneous information conveyed by propaganda or disinformation, the European Union intends not only to deconstruct the manipulation of information and promote a positive vision of Europe by promoting more moderate voices, but also to train citizens to resist internally the attempts of biased and erroneous discourse40. The current structure leaves many relevant issues for co-regulation: all the detailed undertakings imposed on digital intermediaries the Code of Practice are not enforceable at any level, whereas the sanctioning system applies only to some obligations set forth by the DSA. In fact, the voluntary nature of the Code of Practice does not promote a concrete structured cooperation between platforms, that are not subject to material sanctions for implementation failures, apart from the risk of a potential expulsion from the Codes. Moreover, the criteria for assessment, often carried out by the signatories themselves, insufficiently addresses the protection of fundamental rights. On the other side, some important aspects of platform responsibilities remain unclear even in the DSA: the cornerstone of liability exemption remains fundamentally unchanged, as the regulation does not envisage general monitoring obligations for digital intermediaries to actively seek facts or circumstances indicating illegal activity. And, above all, it must be underlined that disinformation, although harmful, cannot be labelled as properly illegal: therefore, while the removal of unlawful content entails clear-cut responsibilities, the lack of concrete obligations to remove disinformation leaves wide discretion to providers of digital services. Undoubtfully, there is a need for further debate on how to reconcile the regulation of harmful but legal content with fundamental rights to freedom of expression41: on the issue of cooperation with online platforms, simple transparency obligations with no additional commitments would certainly be compatible with freedom of expression, but insufficient to tackle the phenomenon; however, too rigid, command and control forms of regulation would likely be ineffective and disproportionate42. The incremental approach to regulation (first self-regulation, then co-regulation if needed) proposed by the Commission is meaningful: however, self-regulation should be accurately monitored through the definition of indicators, and the sharing of good practices43.

Although the EU is striving to achieve greater commitment and involvement of providers of digital services at various level in relation to the fight against disinformation, until now it has generally preferred a soft law-oriented approach with few demands and obligations, being digital intermediaries reluctant to assume greater responsibility. This seems to contrast with the logic of securitization of disinformation issues, as explained in the following pages44. In fact, in the last years the EU has been promoting a discourse linking disinformation to security, exceptionality, and geopolitical strategies, but being lax at the same time with the obligations and responsibilities of digital intermediaries45.

4. Disinformation as a Security Issue: The Concept of FIMI and the Countermeasures Against Russian Propaganda

The European Union has become concerned about the danger of disinformation in terms of security for the first time with reference to the Russian annexation of Crimea and Sevastopol, condemned as illegal in the Conclusions of the European Council of 19 and 20 March 201546. On that occasion, the European Council underlined the need to counter Russia's ongoing disinformation campaigns, inviting the High Representative of the Union for Foreign Affairs and Security to draw up an action plan on communication strategy in collaboration with Member States and EU institutions. As a result, the *East StratCom Task Force* was established within the European External Action Service (EEAS)47, with the aim of developing effective communication strategies in promoting the activities of the European Union in Eastern Europe and beyond48. *Task Force South* and *Task Force Western Balkans* were added to this in 2017. *East StratCom* develops communication products and campaigns designed to better explain EU values, interests and policies in the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine) and supports wider EU efforts aimed at strengthening the media environment in the Eastern Partnership countries and beyond, in close

40 Robin M., 2023, p. 5.
41 Shattock E., 2021, p. 4. Various criticisms regarding the DSA are also expressed by Meyer Z., 2022.
42 Renda A., 2018, p. 24.
43 Renda A., 2018, p. 30.
44 This contrast is clearly outlined by Casera-Ripollés and Others, 2023: a dissonance «between a vision of hard power, facing a cardinal threat, and another of soft law, based on voluntarism and minimal intervention in the digital media industry» (p. 8).
45 Casero-Ripollés A. and Others, 2023, p. 8.
46 https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf
47 https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en
48 Colomina C. and Others, 2021, p. 31-32; Robin M., 2023, p. 4.

collaboration with EU institutions, member states and civil society actors. With regard to disinformation, *East StratCom* reports on and analyses disinformation trends, explains and exposes disinformation narratives, and raises awareness of the negative impact of disinformation that originates in pro-Kremlin sources and is disseminated in the Eastern neighbourhood's information space and beyond. *East StratCom*'s flagship project is EUvsDisinfo[49], a multilingual platform established in 2015 to better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood. It comprises a team of experts with a background mainly in communications, journalism, social sciences and Russian studies, engaged in identifying, compiling, and exposing disinformation cases originating in pro-Kremlin media that are spread across the EU and Eastern Partnership countries.

The logic of securitization – consisting of applying security tools and discourses upon an object that was previously not identified as such – emerges with outstanding clarity from the documents produced in the last months. In March 2022 EU Member States adopted an action plan entitled *A Strategic Compass for Security and Defence*[50]*,* that stresses that Foreign Information Manipulation and Interference (FIMI) does not only constitute a threat to democracy, but also to our security: Russia's use of information manipulation and interference in the preparation and execution of its war of aggression against Ukraine demonstrates this and shows how such activity constitutes an integral part of modern warfare. Shortly afterwards, a report released jointly by ENISA[51] and EEAS[52] in December 202253 has underlined the difference between the *unintentional* spread of false and/or misleading information, and the *intentional* manipulation of the information environment. EEAS has also proposed a definition of FIMI as «a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory». In light of broader hybrid threats that cross different domains, EEAS first report on FIMI threats published in February 202354, one year after Russia's full-scale invasion of Ukraine, contains an analysis of 100 FIMI cases (incidents) detected between the 1st of October and 5th of December 2022, 88 of which involving Russia, in order to (i) objectively analyse the behaviour of actors engaged in manipulating the information environment, and (ii) systematically develop and measure disruptive responses, investigate their efficiency, and understand their potentially negative side effects. As explained in the report55, «the notion of FIMI overlaps with the notion of disinformation, but is at the same time narrower and broader: it is narrower in that it only refers to information manipulation by actors foreign to the EU and its member states, thus not applying to domestic sources; it is broader insofar as it does not require the information spread by threat actors to be verifiably false or misleading. The deciding factor for whether something can be considered FIMI is not false or misleading content, but deceptive or manipulative behaviour».

In parallel the European Parliament, in its resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation56, among an extensive list of security issues labelled foreign interference, information manipulation and disinformation as a serious violation of the universal values and principles on which the Union is founded (par. A) and an abuse of the fundamental freedoms of expression and information (par B.), qualified them as attacks that are part of a hybrid warfare strategy and constitute a violation of international law (par. E), called upon the duty of the EU and its Member States to defend all citizens and infrastructure, as well as their democratic systems, from foreign interference attempts (par. L), recalled that the resilience and preparedness of EU citizens vis-à-vis foreign interference and information manipulation are the first priority of EU defence (par. O), deplored that there is an overall lack of a security culture in the EU institutions despite the fact that they are clear targets (par. BV and 107) for all types of hybrid threats and attacks by foreign state actors.

On 10 March 2022 the European Parliament established a new Special Committee (ING-2) on foreign interference in all democratic processes in the European Union, including disinformation, and the strengthening of integrity, transparency and accountability in the European Parliament. On 1st June 2023, the ING2 report on foreign interference in

[49] *https://euvsdisinfo.eu/*
[50] *https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf*
[51] *The EU agency for cybersecurity.*
[52] *EU external action service.*
[53] *https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape*
[54] *https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf*
[55] *On p. 25.*
[56] *2020/2268(INI). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html*

all democratic processes in the European Union, including disinformation (EP resolution 2022/2075(INI))57 was adopted in plenary. Among the many issues dealt with by this resolution, the EP underlined that Russia's war of aggression against Ukraine brought to the fore the links between attempts at foreign manipulation of information and threats to the EU and its immediate neighbourhood, especially Western Balkans and Eastern Partnership countries, as well as to global security and stability (par 1). Therefore, it expressed the need to move from a country-agnostic approach that treats all foreign influence efforts in the same way, regardless of their source country, towards a risk-based approach based on objective criteria (par. 6) and above called on the Member States to acknowledge the fact that foreign interference, including disinformation, is a national and cross-border security threat and stressed the need for Article 222 TFEU to be amended to include foreign interference. Notably, Article 222 TFEU – included in part five of the Treaty, the one dedicated to the EU's external action – contains the so-called "solidarity clause" binding Member States to mobilize every instrument at their disposal, including military resources, for mutual aid in the event of (for now) terrorist attacks or natural or man-made disasters. The implementation of such obligation, in line with the decision-making procedure typically displayed in the CFSP sector, envisages a decision adopted by the Council acting on a joint proposal by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, of which the European Parliament should be simply informed.

Probably the clearest example of the fact that disinformation has become a CFSP issue, is the Council regulation (EU) 2022/350 of 1st March 202258, based on Council decision (CFSP) 2022/351 of 1st March 202259, both concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine60. This is a concrete case of coordination between a CFSP act – the Council decision – pursuing foreign policy purposes through the intergovernmental decision-making method and another act - the regulation - that concerns the material competences of the Union provided for by the TFEU, in this case those in the field of broadcasting of audiovisual content, information society services and electronic communications. The decision of the Council, whose legal basis is Article 29 TEU61, prevented some Russian media outlets – namely Russia Today English, Russia Today UK, Russia Today Germany, Russia Today France, Russia Today Spanish, and Sputnik – from any possible broadcasting activity by any means, including Internet platforms. The Council regulation, whose legal basis is Article 215 TFEU62, envisaged the same provisions, adding the prohibition of circumventing them, even by acting as substitutes for natural or legal persons, entities or bodies. In the Whereas the Russian Federation is explicitly accused of propaganda actions that constitute a significant and direct threat to the Union's public order and security and the media outlets mentioned in the regulation are labelled as essential and instrumental in bringing forward and supporting the aggression against Ukraine, and for the destabilisation of its neighbouring countries. The issue of the legal basis of both acts is significant. In fact, as stated in Article 24 TUE, par. 2, the adoption of legislative acts in the domain of CFSP is excluded, therefore neither the decision nor the regulation of 1st March 2022 can be considered legislative acts, although binding for EU Member States. Consequently, the use of this type of act to affect the area of freedom of expression and information does not appear to be compatible with Article 10 ECHR, par. 2, which – as is well known – requires that any restrictions on that freedom be prescribed by law63.

The Regulation was challenged by Russia Today France in front of the EU General Court which in a lengthy decision64 rejected the claim and confirmed the Regulation. The Court highlighted «the exceptional context and the

---

57 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.html

58 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0350

59 https://eur-lex.europa.eu/eli/dec/2022/351

60 These acts are commented by Ciliberti L., 2022, Di Turi C., 2022, Lattanzi S., 2022..

61 Article 29 TEU, comprised among the specific provisions of the Treaty concerning CFSP, states that the Council shall adopt decisions which shall define the approach of the Union to a particular matter of a geographical or thematic nature, and that Member States shall ensure that their national policies conform to the Union positions.

62 Article 215 TFEU allows the Council, acting by a qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the Commission and informing the European Parliament, to implement decisions adopted within the CFSP framework, by interrupting or reducing relations with third countries or adopting restrictive measures against natural or legal persons and groups or non-State entities.

63 However, already previously (Judgment of the General Court (Ninth Chamber) of 15 June 2017, Kiselev v Council of the European Union, case T-262/15) the approach of the General Court has been to consider the requirement of the law underlying the restrictive measures to be satisfied, when such measures were adopted with legislative acts of general scope, provided of a clear legal basis, subject to judicial review and in line with the requirements of proportionality and necessity.

64 Judgment of the General Court in Case T-125/22, RT France v Council, 27 July 2022. Press release no. 132/2022 is available here: https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-07/cp220132en.pdf . The judgement is commented by Dunn p., 2023,

extreme urgency in which the contested acts were adopted», that required a rapid response by the EU, consisting of the immediate implementation of the measures decided by the Council, aimed at suspending the activity of a vehicle for propaganda in support of the Russian military aggression. The Court also stressed that this approach «was essential to ensuring the effectiveness of those measures in the light of the objectives that they pursued». It also explained that the Council could not be criticised for having considered that the necessary measures to be taken in response to the serious threat to peace at Europe's borders and the infringement of international law could also include the temporary prohibition on content broadcasting by certain media outlets funded by the Russian State, on the ground that those outlets would support the Russian Federation's military aggression against Ukraine. Notably, on par. 172 of the decision the Russia Today Group is qualified as «an information arm against the Western world». Consequently, the Court concluded that the measures adopted were proportionate appropriate and necessary to the aims pursued, because their nature of temporary and reversible prohibition was compliant with the essential content of the freedom of expression. This case is interesting because it provides a clearly negative answer, at least in emergency contexts, to the question of whether the protection of freedom of expression and information also presupposes freedom of disinformation in its active and passive aspects.

5. Concluding Remarks

Disinformation (and specifically FIMI) has become part of the broader security landscape of contemporary societies. As perfectly outlined by some commentators, «EU's policy against disinformation is based on two opposing logics that coexist and compete. The first is securitization, which understands this problem as a threat to democracy that legitimizes "exceptional decision-making" from a hard power perspective. The second is based on the self-regulation and voluntarism of digital platforms with a clear orientation towards soft law and minimal intervention»65. The EU decision on Sputnik and Russia Today is an example of the ongoing securitization process, where a speech act has been delivered under a logic of exceptionality66. The General Court's ruling on RT France represents a turning point. Indeed, in previous years the EU had viewed disinformation essentially as a danger to the stability of its founding values, which require an environment conducive to democratic public debate. To this extent, over time the EU adopted a series of measures – partly soft law and part hard law – not aimed at criminalizing or banning disinformation, which was considered mostly harmful but not illegal, but at protecting the collective right to be adequately informed. On the contrary, justifying this approach with the rhetoric of emergency, with this ruling the EU has arrogated to itself the right to censor information and news or select their dissemination on reason of their reliability and appropriateness. Indeed, the General Court explicitly denied that the use of mass media for purposes related to the dissemination of propaganda in favor of third countries, especially in the context of an ongoing war conflict, is worthy of strengthened protection as an expression of the freedom of press. This judgment is clearly pervaded by a spirit of "militant democracy". However, it is to be hoped that this tolerance of restrictive forms of freedom of information will not lead to the paradoxical outcome of resorting to dictatorship to defend democracy67.

References

Bayer J. and Others, Disinformation and propaganda: impact on the functioning of the rule of law in the EU and its Member States, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, February 2019.

Bayer J. and Others, Disinformation and propaganda: impact on the functioning of the rule of law in the EU and its Member States. 2021 update, European Parliament, European Parliament, Policy Department for External Relations, April 2021.

Bennett W. L. and Livingston, S., The disinformation order: Disruptive communication and the decline of democratic institutions, in European Journal of Communication, 33(2), 2018, pp. 122-139.

Cabrera Blázquez F. J., The proposal for a European Media Freedom Act, Strasbourg, European Audiovisual Observatory, Decembre 2022.

Casero-Ripollés A. and Others, The European approach to online disinformation: geopolitical and regulatory dissonances, in Humanities and Social Sciences Communications 2023, 10(1):657

Ciliberti L., "Free flow of information" - Il contrasto alla disinformazione in tempi di guerra, in MediaLaws, 2/2022, pp. 349-406.

Sassi S., 2022 and more briefly by Zeno-Zencovich V., 2023. Against this judgement RT France brought an appeal to the Court's Grand Chamber on 27 September 2022 (Case C-620/22 P).

[65] Casero-Ripollés A. and Others, 2023, p. 1.

[66] Casero-Ripollés A. and Others, 2023, p. 7.

[67] Sassi S., 2022, p. 1259.

Colomina C. and Others, The impact of disinformation on democratic processes and human rights in the world, European Parliament, Policy Department for External Relations, April 2021.
Di Turi C., Il conflitto in Ucraina e la "propaganda di guerra" della Federazione russa: quali reazioni da parte dell'Unione europea?, in Eurojus, 2/2022, pp. 327-338.
Dunn P., Il contrasto europeo alla disinformazione nel contesto della guerra in Ucraina: riflessioni a margine del caso RT France, in Medialaws, 1/2023, pp. 201-301.
EEAS – StratCom Division, First Report on Foreign Information Manipulation and Interference Threats, February 2023, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
ENISA and EEAS, Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape, December 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape
European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation - 2020/2268(INI).
European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation - 2022/2075(INI).
Fernandes S., "Security Union" and the digital sphere: unpacking securitization processes, UNIO EU Law Journal, 4/2018, pp 42-47.
High level Group on fake news and online disinformation (HLEG), A multi-dimensional approach to disinformation, European Union, 2018.
Lattanzi S., La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino, in Medialaws, 2/2022, pp. 158-178.
Meyers Z., Will the Digital Services Act save Europe from disinformation?, Centre for European Reforms, 21 April 2022.
Mezzanotte M., "Fake news", "deepfake" e sovranità digitale nei periodi bellici, in Federalismi.it, 33/2022, pp. 44-65.
Pollicino O. and De Gregorio G., Political Advertising and Disinformation: The European Approach, in Medialaws.eu, 28 March 2023.
Renda A., The legal framework to address "fake news": possible policy actions at the EU level, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, June 2018.
Robin M., European Policies in the fight to counter propaganda, in FRS Policy Papers, n. 665, 18 April 2023.
Sassi S., La Soft War dell'Unione europea: il caso RT-France vs. Consiglio, in Il diritto dell'informazione e dell'informatica, 6/2022, pp. 1253-1259.
Shattock E., Self-regulation 2:0? A critical reflection of the European fight against disinformation, in Harvard Kennedy School Misinformation Review, 3, 2021, pp. 1-8.
Wardle C. and Derakhshan H., Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09, 2017.
Zeno-Zencovich V., The EU regulation of speech. A critical view, in Medialaws, 1/2023, pp. 11-18.