The International Lawyer

Volume 53 | Number 2 Article 5

2020

EU Action Plan Against Disinformation: Public Authorities, Platforms and the People

Antonios Kouroutakis

EU Action Plan Against Disinformation: Public Authorities, Platforms and the People

DR. ANTONIOS KOUROUTAKIS[1]

I. Introduction

Democracy is a technology of governance. The spread of democracy—the so called "democratization"—took place progressively and in waves. According to Huntington, the first wave started in 1820, the second with the end of World War II, and the third wave in 1974.[2] Remarkably, before the end of World War II, democracy was close to extinction as only eleven democracies were recorded around the world.[3] Nowadays, democracy is threatened, and a democratic backsliding has occurred.[4] The Freedom House reports that "[i]n 2018, Freedom in the World recorded the 13th consecutive year of decline in global freedom."[5] On top of this, a number of democracies have adopted illiberal reforms, creating a new model of governance between democracy and authoritarianism: the so called "illiberal democracy."[6]

Additionally, there is a widespread feeling of distrust among the people. Interestingly, people express concerns about democracy within even the most established democracies. For instance, a poll published by *The Washington Post* just before the presidential election of 2016 revealed that 40 percent of Americans had "lost faith in democracy."[7]

Furthermore, confidence in democratic institutions has been shaken. According to a Gallup poll, confidence in the United States Congress is very

1. Dr. Antonios Kouroutakis, Assistant Professor at IE University Law School. The author would like to thank the participants in the Lawahead event organized in Madrid under the auspices of IE University in January 2019 entitled "Disinformation as a threat of the upcoming European Elections." All errors remain those of the author.

2. *See* Samuel P. Huntington, *Democracy's Third Wave*, 2 J. OF DEMOCRACY 12, 12 (1991).

3. JOHN KEANE, THE LIFE AND DEATH OF DEMOCRACY, at xxiii (2009).

4. David Waldner & Ellen Lust, *Unwelcome Change: Coming to Terms with Democratic Backsliding*, 21 ANN. REV. OF POL. SCI. 93, 93 – 113 (2018).

5. *Freedom in the World 2019: Democracy in Retreat*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-world/freedom-world-2019/democracy-in-retreat (last visited Feb. 28, 2019).

6. *See* Fareed Zakaria, *The Rise of Illiberal Democracy*, 76 FOREIGN AFF. 22, 24 (1997).

7. *See* Nathaniel Persily & Jon Cohen, *Americans Are Losing Faith in Democracy – and in Each Other*, WASH. POST (Oct. 14, 2016), https://www.washingtonpost.com/opinions/americans-are-losing-faith-in-democracy—and-in-each-other/2016/10/14/b35234ea-90c6-11e6-9c52-0b10449e33c4_story.html?utm_term=.6508ef0e81d5.

low.[8] Likewise, in Europe, according to Eurobarometer, EU citizens' trust in the National Governments and National Parliaments is around twenty-seven percent and twenty-eight percent respectively.[9]

That being said, although democracy has proven to be a very successful form of governance in the twentieth century, at the turn of the twenty-first century it appears to be traumatized. In recent years, a rising threat that endangers democracy is the phenomenon of "disinformation."[10] Information is at the core of the age we are living in, shaping every human activity from the economy to politics, and disinformation and fake news have a tremendous impact on society.

For the purpose of this article, it is necessary to draw a distinction between two terms, "misinformation" and "disinformation," which are often mistakenly used interchangeably. Misinformation is defined as "false information, or [the] dissemination of such information not necessarily in the knowledge that it is false,"[11] while disinformation is "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public"; this may cause public harm.[12]

Both terms indeed overlap, but they do not coincide. The main difference that distinguishes the two concepts is the "intent"; the dissemination of false news *intends* to mislead public opinion.[13] Disinformation is "misinformation by intent." Specifically, the intent must simultaneously cover both the knowledge that the information is false or misleading and, secondly, that the dissemination of such information would be deceiving to the public.[14]

---

8. *See Confidence in Institutions*, GALLUP, https://news.gallup.com/poll/1597/confidence-institutions.aspx (last visited Feb 28, 2019).

9. *See* TNS OPINION & SOCIAL, STANDARD EUROBAROMETER 85 – SPRING 2016: PUBLIC OPINION IN THE EUROPEAN UNION, FIRST RESULTS, at 14 (2016).

10. For criticism on the term "disinformation," *see* JEAN-BAPTISTE JEANGÈNE VILMER ET AL., INFORMATION MANIPULATION: A CHALLENGE FOR OUR DEMOCRACIES 17, 21 (2018) (the authors of the report use instead the term "information manipulation").

11. *Definition of Misinformation*, IATE: EUROPEAN UNION TERMINOLOGY, https://iate.europa.eu/entry/result/3576921/en (last visited June 26, 2019).

12. *Tackling Online Disinformation*, EUR. COMM'N, https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation (last visited Jan. 22, 2020); *see also* HIGH-LEVEL GRP. ON FAKE NEWS & ONLINE DISINFORMATION, EUR. COMM'N, A MULTI-DIMENSIONAL APPROACH TO DISINFORMATION 2, 10 (2018).

13. According to a report issued by the Parliament of Singapore, the actors behind disinformation are categorized among "foreign state actors," "foreign non-state actors," "local actors," or an alignment of different actors, and the causes of disinformation depend on the actor behind the disinformation. Among the causes of disinformation, the report mentions the following: to advance or undermine a domestic or foreign policy, to discredit public institutions and leaders, to achieve an elections outcome, to fracture society's shared reality, to promote or oppose policies or ideological beliefs, to gain financially, and to de-legitimize a government. *See* PARLIAMENT OF SINGAPORE, REPORT OF THE SELECT COMMITTEE ON DELIBERATE ONLINE FALSEHOODS – CAUSES, CONSEQUENCES AND COUNTERMEASURES 29 – 62 (2018).

14. *Id.* at 135.

With disinformation becoming a bigger and bigger problem, the EU, just before the European Elections in 2019, adopted the "EU Action Plan Against Disinformation" (henceforth "Action Plan").[15] This article aims to analyze and evaluate the Action Plan and highlight its core provisions. In doing so, it will first examine briefly both the pathology of disinformation and its impact on democracy and its institutions. Then this article will focus on the Action Plan and its legal framework, focusing on the normative implications as well as the practical application.

This article will argue that the Action Plan was an innovative solution. It was not a top down, hard regulation. On the contrary, it involved every stakeholder concerned in the pathology of disinformation, from social platforms to the common user. Furthermore, the whole framework was a hands-off approach to the problem from the public institutions that hold a supervisory role, while the private entities participated on a voluntary basis. Interestingly, due to its innovative character, the Action Plan was an experiment subject to a twelve-month sunset clause.

II. Disinformation as a Problem: Why the Specific Legal Framework Was a Necessity?

A. Evolution of Disinformation

The word disinformation is modern and originates from the Russian language, in particular from the word "dezinformatsiya," supposedly coined by Joseph Stalin after World War II.[16] During the Cold War, the KGB (the secret service of USSR) spread the rumor that the AIDS virus was created by the Pentagon, the headquarters of the United States Department of Defense.[17] The practice of disinformation, however, has been around since at least the Roman period.[18] It is said that Octavius extensively used disinformation tactics and fake news in order to damage the reputation of Marcus Antonius, painting him as "a womaniser and a drunk, implying he had become Cleopatra's puppet."[19]

Nowadays disinformation has become a growing concern for two main reasons.[20] First, advancement in technology has exacerbated the problem of

15. *Commission Action Plan Against Disinformation*, JOIN (2018) 36 final (Dec. 5, 2018).

16. *See* Adam Tayler, *Before 'Fake News,' There Was Soviet 'Disinformation,'* Wash. Post (Nov. 26, 2016), www.washingtonpost.com/news/worldviews/wp/2016/11/26/before-fake-news-there-was-soviet-disinformation/?utm_term=.dea7ff4dd8e0 ("According to Ion Mihai Pacepa, a high-ranking official in Romania's secret police who defected in 1978, the French-sounding word was invented by Joseph Stalin after World War II.").

17. Vilmer et al., *supra* note 12, at 40.

18. Julie Posetti & Alice Matthews, A Short Guide to the History of 'Fake News' and Disinformation 1 (2018).

19. *See id.* For more historical examples of disinformation, or as the authors call it "information manipulation," *see generally* Vilmer et al., *supra* note 12.

20. In the past, the print and mass media have also accelerated the phenomenon of disinformation. *See* Vilmer et al., *supra* note 12, at 39.

disinformation. Technology to deceive with the support of artificial intelligence (AI) has improved in recent years, specifically "deepfakes." Deepfakes, based on the advances of digital technology and in particular of AI, allow users to create videos presenting somebody to say or to do something in a believable way, even though such persons neither said nor did these actions.[21] Hence, deepfakes have levelled up the technique of disinformation and have created a new dimension to the problem of disinformation where it is almost impossible to distinguish fake videos from originals.[22]

Second, the spread of disinformation is deeply intertwined with the development of digital and social media, such as Facebook and Twitter. Nowadays, anyone, including humans known as "trolls" or algorithms known as "bots," may publish information with few clicks and with the potential to reach online users worldwide.[23] Disinformation via social media may be amplified, targeting a specific group with near instantaneous effects and at a low cost.[24] To exemplify this and compare and contrast it to past incidents of disinformation, it is worth noting that it took four years for the rumor manufactured by the KGB in 1983 that the AIDS virus was created by the Pentagon to reach the Western media.[25]

Furthermore, according to Pew Research Center, more than half of the population in most EU member countries receive the majority of their news from social media platforms, even though this does not reflect the primacy sources through which they receive information.[26] Such practices allow the emergence and expansion of less reliable sources of information.

As a result, disinformation due to technological advancements became a fast-paced and widespread phenomenon evolving together with technology. Disinformation has the potential to be produced in a large scale and in a systematic way distorting public opinion.

B. Disinformation, Defamation, and Intermediary Service Providers: The Incomplete Legal Framework

Nowadays people have the technological means to fabricate disinformation, as well as the means to circulate such disinformation to wider audiences across the world or even to target specific groups. Additionally, these people use anonymity on the internet or even form fake

21. Grace Shao, *What 'Deepfakes' Are and How They May Be Dangerous*, CNBC (Oct. 13, 2019), https://www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html.

22. For more details on deepfakes, *see* Robert Chesney & Danielle Citron, *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, Foreign Affairs (Jan./Feb. 2019), www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

23. For more details, *see* Vilmer et al., *supra* note 12, at 83 – 84.

24. *See* Parliament of Singapore, *supra* note 15, at 14, 20.

25. Vilmer et al., *supra* note 12, at 40.

26. Amy Mitchell et al., *In Western Europe, Public Attitudes Toward News Media More Divided by Populist Views Than Left-Right Ideology*, Pew Res. Ctr.: Journalism & Media (May 14, 2018).

identities in order to protect themselves from legal actions.[27] At the same time, while users can hide behind internet anonymity, the legal framework regarding the limited liability of an intermediary service provider in the U.S. and EU exacerbates the problem, as no one is accountable for the disinformation.

Specifically, in the U.S., Section 230 of the Communications Decency Act of 1996[28] immunizes from liability intermediary service providers on the Internet—on which illegal activities such as defamation or hate speech take place—for statements published by third parties and users. In practice, this means that only the users are liable for illegal activities on the web, and if their identity cannot be determined, then nobody is held accountable.[29]

In the EU, the legal framework is a bit more complex as an intermediary service provider, such as social platforms like Facebook or Twitter, enjoys relative immunity from liability. In particular, apart from the users, who are liable under specific circumstances (primary liability), intermediary service providers on the Internet are liable in instances where they are aware of any unlawful activities (secondary liability).[30] The legal framework at the European level is based on the "Directive on Electronic Commerce."[31] However, the Member States compliment this legal framework with more

27. In particular, such actions, such as the intentional dissemination of lies that can hurt someone fall within libel or defamation and are dealt with in the Civil Code or Criminal Code of a number of jurisdictions.

28. Communications Decency Act of 1996 47 U.S.C. § 230 (1996). In practice, this section overturned the precedent from Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995). In this early case, the court held that held that intermediary service providers could be held liable for the illegal activities, such as unprotected speech, of their users.

29. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003).

30. For more details about secondary liability, see GIOVANNI SARTOR, PROVIDERS LIABILITY: FROM THE ECOMMERCE DIRECTIVE TO THE FUTURE 4 (2017).

31. Directive 2000/31/Ec, of the European Parliament and of the Council of 8 June 2000 On Certain Legal Aspects of Information Society Services, In Particular Electronic Commerce, In The Internal Market (Directive On Electronic Commerce), 2000 O.J. (L 178) 1. In particular Article 14(1) and (3) of Directive 2000/31, entitled "Hosting," provides: "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. . . . 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information." *Id.* art. 14(1)-(3), at 13. In addition Article 15(1) of Directive 2000/31, entitled "No general obligation to monitor," provides: "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity." *Id.* art. 15(1), at 13.

specific provisions.[32] Moreover, the extent of the obligations from the intermediary service providers on the Internet is not well defined.[33]

C. Disinformation as a Danger to Democracy

In democracies, people (demos in Greek) hold the power (kratos in Greek). When people elect their representatives from a number of candidates, such power is temporarily transferred to their elected representatives. Thus, the quintessence of democracy is a system of trust and accountability. Such power is returned to the people every time elections are held and people periodically evaluate their representatives and hold them accountable for their actions and omissions. If people are not satisfied with their representatives, they can always replace them with their competitors.

For democracy to function in a proper manner, it is important that people are able to actively participate and vote based on trustworthy, accurate, and complete information. Thus, a key ingredient for a functional relationship between the people and their representatives (or their competitors) is information. Information allows people to form their political views and draw conclusions about which candidate can serve their best interests.

A fortiori, during electoral periods information might have a decisive impact on the electoral result. Suffice to mention here the bombings of March 11, 2004, in Madrid, Spain.[34] During the electoral period, the controversial topic between the Government of the Popular Party (PP) and the opposition of PSOE was the participation of Spanish troops in the War in Iraq.[35] When a terrorist attack took place killing 193 people and leaving nearly 2,000 injured, despite the evidence that the terrorist attack was associated with a jihadist cell of Al Qaeda, the Government put the blame on the Basque separatist group ETA.[36] When the truth was revealed, the public "turned against the PP government, in large part because Spain had

32. *See Commission White Paper on Illegal and Harmful Content on the Internet*, at 13, COM(96) 487 final (Oct. 16, 1996) ("In a number of Member States (Austria, Germany, France, UK), legislation has been adopted or proposed defining the legal responsibilities of host service providers in such a way that they are only liable for an item of content hosted on their server where they can reasonably be expected to be aware that it is prima facie illegal or fail to take reasonable measures to remove such content once the content in question has been clearly drawn to their attention.").

33. *See, e.g.*, Case C-18/18, Eva Glawischnig-Piesczek v.Facebook Ireland Ltd., http://curia.europa.eu/juris/liste.jsf?num=C18/18# (pending). In this case it is not clear to what extent Facebook must delete all hate postings and verbatim re-postings against Austria's Green party leader, Eva Glawischnig, and whether Facebook must delete the post just in Austria or worldwide.

34. Patricia Ortega Dolz, *"The Government Asked Me to Accept Their Lie About the Madrid Train Bombings,"* El Pais (Mar. 12, 2019), https://elpais.com/elpais/2019/03/12/inenglish/1552403746_691872.html

35. *Id.*

36. *Id.*

supported the United Kingdom and the United States in launching the 2003 war in Iraq."[37]

Misinformation and disinformation distort democratic regimes and bedevil policy makers around the world. However, disinformation is harmful largely because the information is intentionally fabricated and tailored to mislead and deceive, with the aim to enhance the polarization of public views and to interfere in decision-making processes. Conversely, misinformation is a low-risk problem because it is provisionally based on honest mistakes made by journalistic and political actors.

Recently there has been a plethora of orchestrated disinformation incidents around the world.[38] First, disinformation became an issue during the 2016 United States Presidential Elections. "Special Counsel Robert Mueller's 448-page [report] thoroughly detailed how the Russians set up fake social media accounts to spread misinformation that reached 'tens of millions of US persons.'"[39] Furthermore, during the French Presidential Elections in 2017 (a polarized race between Emmanuel Macron and Marine Le Pen), a series of orchestrated disinformation campaigns targeted the former presidential candidate—the so called "Macron Leaks."[40] Among the numerous fabricated stories, it was falsely revealed, in a very sophisticated manner, that Macron's campaign was funded by foreign sources.[41] That being said, it is important to remark that in times of decisive elections or in periods of tension with all the emotions involved therein, people are generally more willing to believe any story that favors their beliefs.

All of the above-mentioned cases, despite each being unique in their own way, have a common denominator. Trust is diminished in the political actor(s) involved whether it be in governments, institutions such as parliaments, candidates, or the news media.[42] As a result, a Eurobarometer survey conducted in February 2018 found eighty-three percent of citizens in the EU believe that disinformation is a danger to democracy.[43] Likewise, across the pond, Pew Research Center found that sixty-eight percent of

37. *Id.*

38. PARLIAMENT OF SINGAPORE, *supra* note 15, at 5 – 13 (2018).

39. Sabrina Siddiqui, *Half of Americans See Fake News as Bigger Threat than Terrorism, Study Finds*, THE GUARDIAN (June 7, 2019), https://www.theguardian.com/us-news/2019/jun/06/fake-news-how-misinformation-became-the-new-front-in-us-political-warfare.

40. VILMER ET AL. *supra* note 12, at 106.

41. It is remarkable that the disinformation campaign was sophisticated, as the site on which the story appeared was a perfect copy of that of a Belgian newspaper "Le Soir" but with a different URL. The official website of Le Soir quickly denied that the story had come from their newsroom. *See Fausse information sur Macron: <Le Soir> victime de plagiat* [*False Information About Macron: "Le Soir" Victim of Plagiarism*], LE SOIR (Mar. 2, 2017), https://www.lesoir.be/art/1451991/article/actualite/france/2017-03-02/fausse-information-sur-macron-soir-victime-plagiat.

42. Andrés Ortega, *A Time of General Distrust*, REAL INSTITUTO ELCANO (Oct. 24, 2017), https://blog.realinstitutoelcano.org/en/a-time-of-general-distrust/.

43. TNS POLITICAL & SOCIAL, FLASH EUROBAROMETER 464: FAKE NEWS AND DISINFORMATION ONLINE 4 (2018).

Americans believe that fake news enhances their distrust in the government, while half of them believe that fake news is a bigger threat to the country than terrorism, illegal immigration, violent crime, or racism.[44]

III. EU Action Plan: Soft Law, Self-Regulation, and Temporary

The aforementioned incidents in the U.S. and France alarmed policy makers in the EU ahead of the European Parliament elections in May 2019.[45] The European Commissioner for Security, Julian King, stated in the American newspaper POLITICO that EU officials are worried that, "given the dispersed nature and comparatively long duration of the European Parliament elections, they present a tempting target for malicious actors."[46]

In light of the upcoming European Parliament elections in May 2019, as well as the national and local elections in Member States in 2020, the Commission developed and adopted the "Action Plan against Disinformation" on December 5, 2018, to ensure that the democratic process will not be distorted by disinformation.[47] The Action Plan offers a holistic approach to face disinformation and in particular is focused on four core areas: improved detection of disinformation; coordinated responses to disinformation; cooperation with online platforms and the industry; and, finally, raising awareness amongst citizens.[48]

In regard to improved detection, analysis, and exposure of disinformation, the Commission decided it was necessary to "strengthen the Strategic Communication Task Forces and Union Delegations through additional staff and new tools which are necessary to detect, analyze and expose disinformation activities."[49] Hence, the budget was significantly increased from 1.9 million Euros in 2018 to 5 million Euros in 2019.[50] In addition, Member States were urged to act at a national level by allocating resources to national agencies.[51] To facilitate prompt reaction to disinformation threats, the Commission decided to establish a Rapid Alert System and

44. Amy Mitchell et al., *Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed*, PEW RES. CTR.: JOURNALISM & MEDIA (June 5, 2019), https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/.

45. However, it is noteworthy that the EU officials since 2015 have spotted the issue of disinformation. *European Council Meeting (19 and 20 March 2015) – Conclusions, Brussels* (Mar. 20, 2015), EUCO 11/15, CO EUR 1, CONCL 1, https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.

46. Laurens Cerulus, *Europe's most hackable election*, POLITICO (Jan.16, 2019), www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation.

47. *Commission Action Plan Against Disinformation*, at 2, JOIN (2018) 36 final (Dec. 5, 2018).

48. *Id.* at 5.

49. *Id.* at 6.

50. *Id.*

51. *Id.*

encouraged Member States to share intelligence via fact-based and effective communication in order to counter and face disinformation.[52]

The former two parts of the action plan were mainly activities undertaken by public institutions—EU bodies as well as Member State bodies. However, the third part set forth a framework for key players, such as social media platforms, browser and web platforms, and the advertising industry, in enabling the dissemination of online disinformation.[53] In particular, the main online platforms, such as Google, Facebook, Youtube, and Twitter; the providers of software, namely Mozilla; advertisers and trade associations representing online platforms; and the advertising industry signed the "Code of Practice" on Disinformation published on September 26, 2018.[54] According to the Code of Practice, the relevant industry should immediately "(i) ensure scrutiny of ad placement and transparency of political advertising, based on effective due diligence checks of the identity of the sponsors, (ii) close down fake accounts active on their services and (iii) identify automated bots and label them accordingly."[55]

In addition, the Code of Practice included an Annex with best practices from the signatory members.[56] Examples of these practices include the Facebook policy to remove fake accounts associated with the spread of disinformation or Facebook tools to report fake news, the Google policy to prohibit the placement of advertisements in pages that have misleading content, the Twitter policy regarding transparency in advertisements and the YouTube policies blocking spam videos.[57]

Furthermore, the Code of Practice includes several "Key Performance Indicators" that aim to measure and monitor the efforts taken by the signatories.[58] Overall, the Commission has the ability to monitor signatories' compliance with the Code of Practice by administering comprehensive evaluations for an initial twelve-month period.[59]

Finally, the fourth part of the action plan deals with raising awareness amongst the people/civil society.[60] People are both the victims of disinformation and, at the same time, the vehicle spreading false information. EU policy makers acknowledge the significance of the people in building an effective and resilient mechanism against disinformation, which is why they worked to move the people from the heart of the problem

52. *Id.* at 7.

53. *Id.* at 8.

54. *Code of Practice on Disinformation*, EUR. COMM'N (Sept. 26, 2018), https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

55. *Commission Action Plan Against Disinformation*, at 8 – 9, JOIN (2018) 36 final, (Dec. 5, 2018).

56. *Annex II: Current Best Practices From Signatories of the Code of Practice* (2018), https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

57. *Id.*

58. *EU Code of Practice on Disinformation*, § III (2018), https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (follow "The Code" hyperlink).

59. *Id.*

60. *Commission Action Plan Against Disinformation*, at 10, JOIN (2018) 36 final, (Dec. 12, 2018).

to the core of the solution. These EU institutions have worked with Member States to raise awareness by organizing campaigns and trainings for media and public-opinion shapers.[61] Furthermore, they are committed to supporting the creation of independent bodies and researchers whose role would be to detect and expose disinformation campaigns.[62]

By raising awareness about the threats from disinformation, and by improving citizens' media literacy on how to double check the reliability of information online, the whole edifice against disinformation was enriched with a more holistic dimension against disinformation. According to the fourth pillar of the EU Action Plan, even though people are both the victims and the vehicle for disinformation, with education they can be the fact checkers of information and the ultimate protectors of the truth.

IV. EU Action Plan: An Assessment

Regulators around the world have the option to regulate and tackle disinformation or to ignore it. Regarding the latter, the assumption is that truth always prevails and facts win over fiction. Moreover, disinformation in the end will create a backlash and will produce the exact opposite result. There are two key difficulties in regulating disinformation: first, who has the authority to decide what is truth and what is falsehood and second, there is always the danger that regulators will adopt strict laws that will have a disproportionate impact regarding the freedom of speech.

A fortiori, the fight against disinformation poses some core challenges because of the nature of falsehood in combination with the internet era. Truth is challenged by falsehood, and a competition emerges regarding which side of the story, the true or the false, will prevail. People tend to accept what complies with their views and expectations as the truth.[63] Orchestrated disinformation campaigns exacerbate this problem. The widespread and repetitive reference of falsehoods by a plethora of users takes advantage of human tendencies to believe and accept as truth what a broader group of people claim.[64] The impact of this disinformation is hard to evaluate. Disinformation may have immediate an effect by discrediting a candidate during elections, thus distorting the electoral process. Moreover, disinformation may have a long-term impact by forming false perceptions and illusions that incrementally harm the reputation of democratic institutions, individuals, and businesses.

---

61. *Id.* at 11.

62. *Id.*

63. Ana Lucia Schmidt et al., *Anatomy of News Consumption on Facebook*, 114 PROC. NAT'L ACAD. SCI. 3035, 3035 (2017), www.pnas.org/content/pnas/114/12/3035.full.pdf.

64. *See* Danielle C. Polage, *Making Up History: False Memories of Fake News Stories*, 8 EUR. J. PSYCHOL. 245, 245 (2012), https://ejop.psychopen.eu/article/view/456/pdf; Lisa K. Fazio et al., *Knowledge Does Not Protect Against Illusory Truth*, 144 J. EXPERIMENTAL PSYCHOL. 993, 993 (2015). www.apa.org/pubs/journals/features/xge-0000098.pdf.

Besides the inherent challenges that come with disinformation in the internet era, the EU institutions had to conceive, adopt, and implement an action plan within a tight time framework. EU elections were looming, and it was necessary for the EU Action Plan to include measures to be taken in the short- and medium-term. As of today, this Action Plan is the most concrete and specific initiative on the matter. The EU Action plan was intended to be an immediate reaction to deter disinformation. In practice, it was a joint action in the right direction. It strengthened cooperation between all parties involved—public bodies, platforms, the people, and the civil society. As was seen in Part A, disinformation is a problem with diverse and complicated roots and severe impacts on democracy and its institutions; therefore, the role of countering disinformation cannot and should not be limited to any one single action plan or governing body.

It would have been problematic if the EU Action Plan centralized the efforts against disinformation within the boundaries of the public bodies. A very strict regulatory framework would have restricted what people can do on social platforms, and thus it would have oppressed their innovative character. Furthermore, only in authoritarian and illiberal regimes is the government empowered with the "correct side of the story" while the press and the opposition are silenced. Thus, it was rightly decided that the role of the public was to supervise the implementation of the plan.[65]

The innovative character of this Action Plan, and its Achilles' heel, was its soft law approach. The action plan was a modest and hands-off approach from the perspective of the public bodies, as it framed voluntary obligations for the private entities, especially for social media and other similar industries. At the same time, the hands-off character of the Action Plan was its Achilles' heel because its success depended heavily on the voluntary cooperation of every stakeholder. For that purpose, the Action Plan was a time limited experiment, and it was emphatically stressed "should the implementation and the impact of the Code of Practice prove unsatisfactory, the Commission may propose further actions, including actions of a regulatory nature."[66]

Indeed, the Code of Practice was subject to a twelve-month limitation (sunset clause)[67] which signals the experimental character of the Action Plan. On the top of that, it signals the intention of the public bodies to closely monitor the application of this Action Plan and to take extra measures if they consider it necessary. Indeed, reports from the first months, namely January

65. *See Code of Practice on Disinformation*, *supra* note 56 ("Between January and May 2019, the European Commission carried out a targeted monitoring of the implementation of the commitments by Facebook, Google and Twitter with particular pertinence to the integrity of the European Parliament elections.").

66. *Commission Action Plan Against Disinformation*, at 9, JOIN (2018) 36 final, (Dec. 12, 2018).

67. Regarding the experimental use of sunset clauses, *see generally* ANTONIOS KOUROUTAKIS, THE CONSTITUTIONAL VALUE OF SUNSET CLAUSES: A HISTORICAL AND NORMATIVE ANALYSIS (2017); SOFIA RANCHORDÁS, CONSTITUTIONAL SUNSETS AND EXPERIMENTAL LEGISLATION; A COMPARATIVE PERSPECTIVE (2014).

and February, were heavily criticized by the EU Commission, which demanded more intense efforts.[68]

Because it is difficult to measure the impact of disinformation—for instance, to what extent people are eventually influenced in their lives by fake news—it is equally difficult to measure the impact of a policy against disinformation. The safest way to evaluate the Action Plan is ex post. First, the voluntary character of the EU Action Plan was proven successful.[69] Most of the stakeholders involved in disinformation—from social platforms to internet providers, and from governmental agencies to the people—complied with the provisions of the Action Plan.[70]

Second, it is equally important to stress than no major orchestrated disinformation incidents took place during the EU elections. Actually, in January 2019, Microsoft prevented a preliminary disinformation action by a group of hackers called "Fancy Bear."[71] This group, believed to be associated with Russian intelligence, targeted email accounts of European think tanks and NGOs.[72] This implies that either the preventive nature of the Action Plan deterred the actors behind disinformation or it successfully blocked them.

However, although the Action Plan is the first concrete response to disinformation with innovative and promising provisions, it has clear drawbacks and limitations. First, the EU Action Plan was focused on the looming elections, thus neglecting the long-term dimension of disinformation. As it was mentioned above, disinformation may not have an immediate impact but instead may little by little discredit the truth and form illusions and false perceptions with a long-term impact. In addition, it targeted the major social platforms and internet providers, leaving less important platforms outside of its scope.

Third, the EU Action Plan over relied on self-regulation and self-policing, which is not always efficient. For instance, Facebook introduced the policy "Why I am seeing this ad," which aimed to comply with the provision of the Code of Practice that recognized the importance of "enabling users to understand why they have been targeted by given advertisement."[73] Although this policy increased the transparency in the social platforms and the awareness of the users about how social platforms

68. European Commission Press Release IP/19/746, Code of Practice Against Disinformation: Commission Calls on Signatories to Intensify Their Efforts (Jan. 28, 2019); European Commission Press Release IP/19/1757, Code of Practice Against Disinformation: Commission Takes Note of the Progress Made by Online Platforms and Urges Them to Step up Their Efforts (Mar. 19, 2019).

69. European Commission Press Release IP/19/746, Code of Practice Against Disinformation: Commission Calls on Signatories to Intensify Their Effort (Jan. 28, 2019).

70. *Id.*

71. *Russia Is Not Interfering in the EU Elections*, EU VERSUS DISINFORMATION (Mar. 11, 2019), https://euvsdisinfo.eu/report/russia-does-not-interfere-into-the-eu-elections/.

72. *Id.*

73. *EU Code of Practice on Disinformation*, *supra* note 60, § II.B.

and advertisers use their data , it seems that this policy is missing significant amounts of crucial information.[74]

Furthermore, the EU Action Plan granted discretion to social platforms to regulate free speech and control public debate. As a result, these platforms had unchecked power to decide the content of free speech and even to deactivate user profiles. A U.N. Joint Declaration on fake news from 2017 has identified that "[g]eneral prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information,' are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished."[75] This declaration encapsulates the general concern about the fine line between free speech and its disproportionate oppression. Having said that, a more permanent framework is necessary. Such a framework needs to include more specific regulations about the role and the obligations of all social platforms and internet providers.

V. Conclusion

This article has examined the issue of disinformation. It explored its evolution and remarked on the escalation of the problem due to technological advancements. As disinformation affected the quality of our democracy, policy makers had to step in. The first and concrete effort to regulate disinformation was taken by EU policy makers. Specifically, just before the European Elections in May 2019, the EU Commission adopted and implemented the European Action Plan against disinformation. This Action Plan was a modest regulatory intervention, which was based on soft law and self-regulation.

The action plan was focused on four core areas: the improved detection of disinformation, the coordinated responses of disinformation, cooperation with online platforms and the industry, and finally on raising awareness amongst citizens and developing resilience in the society. The success of the action plan was based on cooperation between public authorities, social media and browsing platforms, and the people.

Public authorities had mainly a supervisory role. To do so they increased their regulatory budget from 1.9 million Euros in 2018 to 5 million Euros in 2019.[76] Furthermore, the Action Plan imposed a set of obligations on social platforms and internet providers such as periodic reporting and measures taken on their behalf to prevent and block disinformation incidents and

74. Among others, Facebook does not inform how it uses data to infer information about users and how exactly an advertiser is then able to reach a user. For more details, *see Why Am I Seeing This on Facebook? It's Still Unclear*, PRIVACY INT'L (Apr. 1, 2019), https://privacyinternational.org/news/2772/why-am-i-seeing-facebook-its-still-unclear.

75. *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda*, ORG. FOR SEC. AND CO-OPERATION IN EUR. (Mar. 3, 2017), www.osce.org/fom/302796?download=true.

76. *Commission Action Plan Against Disinformation*, at 8, JOIN (2018) 36 final (Dec. 5, 2018).

actors. Finally, the Action Plan focused on how public authorities and platforms can raise awareness with the public and improve their media literacy.

In essence, the Action Plan was an innovative regulatory framework. It was a hands-off approach from the perspective of the public institution, it was on a voluntary basis with no hard law obligations, and finally it was experimental for twelve months. Ex post, the Action Plan was a successful regulatory intervention. No major disinformation incidents occurred during the electoral period and all parties cooperated in order to achieve the goals of the Action Plan. Having said that, based on the results of the Action Plan, a more permanent framework is necessary, as disinformation seems to be an omnipresent threat requiring more concrete obligations on behalf of the social media platforms and internet providers.