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

Dr. Antonios Kouroutakis, Assistant Professor IE University
akouroutakis@faculty.ie.edu

Abstract

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. But this system of trust is distorted by disinformation which became a fast-paced and widespread phenomenon. A foriori, during electoral periods, disinformation might have a decisive impact on the electoral result. A number of incidents of orchestrated disinformation around the world, alarmed the policy makers in the EU ahead of the European Parliament elections in May 2019 and the EU Action Plan Against Disinformation was adopted.

This Action Plan is the most concrete and specific initiative on the matter. It is a modest regulatory intervention, based on soft law and self-regulation. As it is subject to a 12 month sunset clause, this marked its experimental nature and the EU Commission's effort to monitor closely its application. The success of the action plan was based on the cooperation of the public authorities, of the platforms and the people. In substance, it was focused on four core areas: first on the improved detection of disinformation, second on the coordinated responses of disinformation, third on the cooperation with online platforms and the industry, and finally on the raising awareness and building resilience amongst citizens.

Introduction

Democracy is a technology to govern. The spread of democracy, the so called 'democratization', took place progressively, with 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.[1] Remarkably, before World War II, democracy was close to extinction as only eleven democracies were recorded around the world. Nowadays, such technology is threatened and a democratic backsliding has occurred.[2] The Freedom House reports that '[i]n 2018, Freedom in the World recorded the 13th consecutive year of decline in global

[1] *See* Samuel P. Huntington, "Democracy's Third Wave" [1991] 2 Journal of Democracy 12.
[2] David Waldner and Ellen Lust, "Unwelcome Change: Coming to Terms with Democratic Backsliding" [2018] 21 Annual Review of Political Science 93.

freedom'.[3] 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.[4]

In addition, among the people a feeling of distrust is wide spread. Interestingly, people express concerns about democracy among the most established democracies. For instance, a poll published by The Washington Post just before the presidential election of 2016 revealed that forty per cent of Americans had 'lost faith in democracy'.[5]

Furthermore, the confidence in democratic institutions has been shaken. According to the Gallup levels of confidence, which runs for 40 years, the US Congress receives very low appreciation rates.[6] Likewise, in Europe, according to Eurobarometer, among EU citizens the trust in the National Governments and National Parliaments is around 27 per cent and 28 per cent respectively.[7]

Having said this, although democracy has proven to be a very successful form of governance in the 20th century, at the turn of the 21st century it appears to be traumatized. In recent years, a rising threat that endangers democracy is the phenomenon of 'disinformation'.[8] Information is at the core of the age we are living in, shaping every human activity from the economy to politics. E contrario, disinformation and fake news have a tremendous impact.

For the purpose of this paper, it is necessary to draw a distinction between two terms, 'misinformation' and 'disinformation', which are often mistakenly used interchangeably. Misinformation is the 'false information, or dissemination of such information not necessarily in the knowledge that it is false'[9] while disinformation is 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.'[10]

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.[11] Disinformation is the 'misinformation by intent'. Specifically

---

[3] Freedom House Report 2019, 'Democracy in Retreat' <https://freedomhouse.org/report/freedom-world/freedom-world-2019/democracy-in-retreat> accessed 28 February 2019.

[4] *See* Fareed Zakaria, "The rise of illiberal democracy" [1997] 76 Foreign Affairs 22.

[5] *See* Nathaniel Persily and Jon Cohen, "Americans are losing faith in democracy — and in each other" (Washington Post, 14 October 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 accessed 28 February 2019.

[6] *See* <https://news.gallup.com/poll/1597/confidence-institutions.aspx> accessed 28 February 2019.

[7] *See* Standard Eurobarometer 85 Spring 2016 [14].

[8] For criticism on the term 'disinformation' see Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume and Janaina Herrera, "Information Manipulation, A Challenge for our Democracies" (Report by the Policy Planning Staff and the Institute for Strategic Research of France, August 2018) <https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf>. The authors of the report use instead the term 'information manipulation' *see* at [21].

[9] 'Misinformation', Interactive Terminology for Europe (2012) <https://iate.europa.eu/entry/result/3576921/en> accessed 26 June 2019.

[10] Report of the Independent High Level Group on Fake News and Online Disinformation, "A multi-dimensional approach to disinformation" (Luxembourg: Publications Office of the European Union, 2018) 10.

[11] 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

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 for the public.

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'). 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 it 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 simple 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, in essence the Action Plan was an experiment subject to a twelve month sunset clause.

A. 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 word 'dezinformatsiya', supposedly coined by Joseph Stalin after World War II.[12] For instance, 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.[13] Disinformation, however, is a practice that has been around since at least the Roman period. 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'.[14]

---

a government. *See* Parliament of Singapore, 'Select Committee on Deliberate Online Falsehoods—Causes, Consequences and Countermeasures' (Presented to Parliament on 19 September 2018) [29-62] <https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport> accessed 26 June 2019.

[12] '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.' *See* Adam Tayler, "Before 'fake news,' there was Soviet 'disinformation'" *The Washington Post* (26 November 2016) <www.washingtonpost.com/news/worldviews/wp/2016/11/26/before-fake-news-there-was-soviet-disinformation/?utm_term=.dea7ff4dd8e0> accessed 10 June 2019.

[13] *See* Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume and Janaina Herrera, "Information Manipulation, A Challenge for our Democracies" (Report by the Policy Planning Staff and the Institute for Strategic Research of France) <https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf> [40] accessed 6 June 2019.

[14] Julie Posetti and Alice Matthews, 'A short guide to the history of 'fake news' and disinformation' (International Center for Journalists, July 2018) <www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf>accessed 4 June 2019. For more historical examples of disinformation, or as the authors call it 'information manipulation' *see* "Information Manipulation, A Challenge for our Democracies" (n 13).

Nowadays disinformation has become a growing concern for two main reasons.[15] First, the advancement in technology has exacerbated the problem of disinformation, since technology to deceive with the support of artificial intelligence (AI) has improved in recent years. Suffice to mention here '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 or did these actions. Hence, deepfakes have levelled up the technique of disinformation and have created a new dimension where it is almost impossible to distinguish fake videos from original.[16]

Second, the wide spread of disinformation is deeply intertwined with the development of digital and social media, such as Facebook and Twitter. Nowadays, anyone, such as humans known as 'trolls' or algorithms known as 'bots', may publish information, with few clicks and with the potential to reach online users worldwide.[17] Disinformation via social media may be amplified, targeting a specific group, with near instantaneous effects and at a low cost.[18] 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 AIDS virus was created by the Pentagon to reach the Western media.[19]

Furthermore, according to Pew Research Center more than half of the population in most member countries of the EU receive the majority of their news from social media platforms while this does not reflect the primacy sources through which they receive information.[20] Such practices allow the emergence and expansion of less reliable sources of information.

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

b. Disinformation, defamation and intermediary service providers: the incomplete legal framework

Nowadays people have the technological means to fabricate disinformation, while they also have the means to circulate such disinformation to wider audiences across the world

[15] In the past, the print and the mass media have also accelerated the phenomenon of disinformation. See (n 13).

[16] For more details on deepfakes see Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War" *Foreign Affairs* (January/February 2019) <www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> accessed 6 June 2019.

[17] For more details *see* (n 13).

[18] *See* Parliament of Singapore, Select Committee on Deliberate Online Falsehoods—Causes, Consequences and Countermeasures (Presented to Parliament on 19 September 2018) <https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport> [66 and 93] accessed 10 June 2019.

[19] *See* (n 13).

[20] Amy Mitchell and others, 'In Western Europe, Public Attitudes Toward News Media More Divided by Populist Views Than Left-Right Ideology' (2018) 202.419.4372 Pew Research Center <www.journalism.org/wp-content/uploads/sites/8/2018/05/PJ_2018.05.14_Western-Europe_FINAL.pdf> accessed 3 March 2019.

or even to target specific groups. On top of that, these people use the anonymity on the internet or even form fake identities in order to protect themselves from legal actions.[21]

At the same time, while users can hide behind the internet anonymity, the legal framework regarding the limited liability of an intermediary service provider in the US and EU exacerbates the problem as no one is accountable for the disinformation.

Specifically in the US, Section 230 of the Communications Decency Act of 1996[22] immunizes from liability intermediary service providers on the Internet in which illegal activities take place such as defamation or hate speech 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 in case their identity cannot be determined, then nobody is held accountable.[23]

In the EU, the legal framework is a bit more complex as an intermediary service provider, such as social platforms like Facebook or Twitter enjoying 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 for instance in case they are aware of any unlawful activities (secondary liability).[24] The legal framework at European level is based on the 'Directive on Electronic Commerce',[25] however, the Member States compliment this legal framework with more specific

[21] 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.

[22] Telecommunications Act of 1996 47 U.S.C. § 230. In practice this section overturned the precedent from the case *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.

[23] *See* for instance *Carafano v. Metrosplash.com*, 339 F.3d 1119 (9th Cir. 2003).

[24] For more details about the secondary liability see Giovanni Sartor, 'Providers Liability: From the eCommerce Directive to the future' European Parliament, Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy (October 2017) http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf accessed 6 June 2019.

[25] 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') OJ L 178, 17.7.2000. 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.' 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.'

provisions.[26] Moreover, the extent of the obligations from the intermediary service providers on the Internet is not well defined.[27]

c. Disinformation as a threat 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 representations 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 foriori, during electoral periods information might have a decisive impact on the electoral result. Suffice to mention here the bombings of March 11 in 2004 in Madrid, Spain. 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. 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. When the truth was revealed, the public 'turned against the PP government, in large part because Spain had supported the United Kingdom and the United States in launching the 2003 war in Iraq'[28]

Although both misinformation and disinformation are a problem distorting the democratic regimes and bedeviling policy makers around the world, disinformation is harmful largely because the information is intentionally fabricated and tailored to mislead and deceive the public or part of it, with the aim to enhance the polarization of public views and to interfere in the decision making processes. On the other hand, misinformation is a low risk problem, as it is provisionally based on honest mistakes made by journalist and political actors.

---

[26] '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.' *See* European Commission, 'Illegal and Harmful Content on the Internet' Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(96) 487 (16 October 1996).

[27] *See for instance* the Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (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.

[28] Patricia Ortega Dolz, "The government asked me to accept their lie about the Madrid train bombings" (*El Pais*, 12 March 2019) https://elpais.com/elpais/2019/03/12/inenglish/1552403746_691872.html accessed 5 June 2019.

Recently there are a plethora of orchestrated disinformation incidents around the world.[29] However, this issue was put in the spotlight due to its intense presence during elections. First, disinformation became an issue during the Presidential elections in the US in 2016. According to 'Special Counsel Robert Mueller's 448-page thoroughly detailed how the Russians set up fake social media accounts to spread misinformation that reached "tens of millions of US persons"'.[30] Furthermore, in Europe during the French Presidential Elections in 2017, which was 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'.[31] Among the numerous fabricated stories, it was falsely revealed, in a very sophisticated manner, that the Macron's campaign has been funded by foreign sources.[32]

That said, it is important to remark that in times of decisive elections or in period of tension with all the emotions involved therein, people in general are willing to believe any story that favors their beliefs.

All of the above-mentioned cases, in spite of each being unique in their own way, have a common denominator; trust is diminished in the political actors involved whether it be in governments, institutions such as Parliaments, candidates, or in the news media.[33] As a result, according to the Eurobarometer survey from February 2018, 83 per cent of citizens in the EU believe that disinformation is a 'danger to democracy'.[34] Likewise, across the pond, according to Pew Research Center, 70 per cent of the Americans believe that fake news enhances their distrust over the government while half of them believe that fake news is a bigger threat to the country than issues such as terrorism, illegal immigration, violent crime or racism.[35]

---

[29] *See* Parliament of Singapore, Select Committee on Deliberate Online Falsehoods—Causes, Consequences and Countermeasures (Presented to Parliament on 19 September 2018) <https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport>

[30] 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> accessed 7 June 2019.

[31] Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, Information Manipulation, A Challenge for our Democracies (Report by the Policy Planning Staff and the Institute for Strategic Research of France) available at https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf [106].

[32] 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* Le Soir, 'Fausse information sur Macron: «Le Soir» victime de plagiat' (*Le Soir*, 2 March 2017) <https://www.lesoir.be/art/1451991/article/actualite/france/2017-03-02/fausse-information-sur-macron-soir-victime-plagiat> accessed 7 June 2019.

[33] Andrés Ortega, 'A time of general distrust' (*Real Instituto Elcano*, 24 October 2017) <https://blog.realinstitutoelcano.org/en/a-time-of-general-distrust/> accessed 2 March 2019.

[34] TNS Political & Social 'Fake News and Disinformation Online' (*Directorate-General for Communication*, April 2018) <http://data.europa.eu/euodp/en/data/dataset/S2183_464_ENG> accessed 7 June 2019.

[35] Amy Mitchell, Jeffrey Gottfried, Galen Stocking, Mason Walker and Sophia Fedeli, 'Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed' (*Pew Research Center*, June 2019) <https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/> accessed 7 June 2019.

B. EU Action Plan: Soft law, self-regulation and temporary

The aforementioned incidents in the US, and France alarmed the policy makers in the EU ahead of the European Parliament elections in May 2019.[36] 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.'[37]

In light of the upcoming European Parliament elections in May 2019, as well as the national and local elections in Member States by 2020, the Commission developed and adopted the 'Action Plan against Disinformation' on December 5, 2018 to secure that the democratic process will not be distorted by disinformation.[38]

The Action Plan aimed to offer a holistic approach to face disinformation and in particular it focused on four core areas: first on the improved detection of disinformation; second on the coordinated responses of disinformation; third on the cooperation with online platforms and the industry, and finally on raising awareness and building resilience amongst citizens.[39]

For the first area, for improved detection, analysis and exposure of disinformation, it was 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'.[40] Hence, the budget was significantly increased from 1.9 million Euros in 2018 to 5 million Euros in 2019. In addition, Member States were urged to act likewise at a national level allocating resources to national agencies.

Regarding the second area, which is about the prompt reaction to disinformation threats, it was agreed that a Rapid Alert System will be established and Member States should share intelligence via fact-based and effective communication in order to counter and face disinformation.[41]

While the former two areas were mainly activities undertaken by the public institutions, EU bodies as well as Member State bodies, the third area set the framework from the perspective of the key players in enabling the dissemination of online disinformation which are the platforms and the social media as well as the advertising industry.

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 26 September 2018.[42] According to the Code of Practice,

---

[36] However, it is noteworthy that the EU officials since 2015 have spotted the issue of disinformation. European Council. Brussels, 20 March 2015. (OR. en). EUCO 11/15. CO EUR 1. CONCL 1 <https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf > accessed 8 June 2019.

[37] Laurens Cerulus, 'Europe's most hackable election' (*Politico*, 16 January 2019) <www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation/> accessed 6 March 2019.

[38] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 2.

[39] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 5.

[40] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 6.

[41] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 6.

[42] 'Code of Practice on Disinformation' (Brussels, 2018) <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> accessed 5 June 2019.

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.'[43]

In addition, the Code of Practice included an Annex with best practices from the signatory members.[44] Among the best practices recorded in the Annex suffice to mention here for instance, 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 with transparency in advertisements and the Youtube policies blocking spam videos.

Furthermore, the Code of Practice includes several 'Key Performance Indicators' that aim to measure and monitor the efforts taken by the signatories. Overall, the Commission had the role to monitor the compliance to the Code of Practice with comprehensive evaluations for an initial 12-month period as an experimental period.

Finally, the fourth area regarding the raising awareness was the legal framework from the perspective of the people, the civil society.[45] 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 and thus they placed the people from the heart of the problem to the core of the solution. The EU institutions have cooperated with Member States in order to raise awareness through organising campaigns and trainings for media and public opinion shapers.[46] Furthermore, they committed to support the creation of independent bodies and researchers with the role to detect and expose disinformation campaigns.[47]

By raising awareness on 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 Actions Plan, people as both the victims and the vehicle for disinformation, were recognized as the fact checkers of information, and the ultimate protectors of the truth.

a. EU Action Plan: An assessment

To begin with, regulators around the world have the option either to regulate and tackle disinformation, or to ignore it. Regarding the latter, the assumption is that truth always prevails and facts win over the fiction. Disinformation in the end will create a backlash and will produce the exact opposite result. Regarding the former two key difficulties in regulating disinformation exist; 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 impact disproportionately with the freedom of speech.

[43] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 8-9.
[44] 'Code of Practice on Disinformation' (Brussels, 2018) [Annex] <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> accessed 5 June 2019.
[45] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 10.
[46] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 11.
[47] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 11.

A fortiori, the fight against disinformation poses some core challenges because of the nature of falsehood in combination with the internet era. In reality, truth is challenged by falsehood and a competition emerges regarding which side of the story, the true or the false, will prevail. According to a study, it seems that people have the tendency to accept what complies with their views and expectations as the truth.[48] Second, orchestrated disinformation campaigns exacerbate this problem. The widespread and repetitive reference of falsehoods by a plethora of users takes advantage of the human tendencies to believe and accept as truth what a broader group of people claim.[49]

Second, it is difficult to evaluate the impact of disinformation. Disinformation may have immediate effect for instance by discrediting a candidate during elections and thus by distorting the electoral process. Moreover, disinformation may have long-term impact by forming false perceptions and illusions that incrementally harm the reputation of democratic institutions, individuals and businesses.

Besides the inherent challenges due to the nature of disinformation in the internet era, the EU institutions had to conceive, adopt and implement an action plan within a tight time framework and time pressure. 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 in deterring 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, with severe impacts on democracy and its institutions and therefore the role of countering disinformation cannot and should not be limited to any one single portfolio.

It would have been problematic if the EU Action Plan has centralized the efforts against disinformation within the boundaries of the public bodies. A very strict regulatory framework would have possibly restricted what people can do on social platforms and thus it would have oppressed their innovative character. Furthermore, only in authoritarian and illiberal regimes, the government is empowered with the 'correct side of the story' while the press and the opposition is silenced. Thus, it was rightly decided that the role of the public was supervisory on the implementation.[50]

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

---

[48] Ana Lucía Schmidt and others, 'Anatomy of news consumption on Facebook' (2017) 114 Proceedings of the National Academy of Sciences of the United States of America <www.pnas.org/content/pnas/114/12/3035.full.pdf> accessed 29 January 2019.

[49] This is called the illusory truth effect. For more details *see* Danielle C. Polage, 'Making up History: False Memories of Fake News Stories' (2012) 8(2) Europe's Journal of Psychology <https://ejop.psychopen.eu/article/view/456/pdf> accessed 16 April 2019. Interestingly, vulnerable to the illusory truth effect are equally people with and without prior knowledge on a subject. *See* Lisa K. Fazio and others, 'Knowledge Does Not Protect Against Illusory Truth' (2015) 144 Journal of Experimental Psychology <www.apa.org/pubs/journals/features/xge-0000098.pdf> accessed 2 April 2019.

[50] '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.' *See* European Commission, 'Code of Practice on Disinformation' COM (Brussels, 2018) page 3 <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> accessed 5 June 2019.

the social media and the relevant industry. 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. Possibly for that purpose, the whole Action Plan was a time limited experiment and it was emphatically stressed in the Action Plan that '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'.[51]

Indeed, the Code of Practice was subject to a 12-month limitation (sunset clause)[52] which signals the experimental character of the Action Plan. On the top of that, it signals the intention of the public bodies to closely the application of this Action Plan and to take extra measures if they consider it necessary. Indeed, reports from the first months, namely January and February, were heavily criticized by the EU Commission, which demanded more intense efforts.[53]

As 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. Primarily, the voluntary character of the EU Action Plan was proven successful. Most of the stakeholders involved in, from social platforms to internet providers, and from governmental agencies to the people, complied with the provisions of the Action Plan.

Second, it is equally important to stress than no major and 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'. This group, believed to be associated with the Russian intelligence, targeted email accounts of European think tanks and NGOs.[54]

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 and concrete response to disinformation with innovative and promising provisions, it has clear drawbacks and limitations to it. 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 as little by little it may 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.

---

[51] Commission, 'Action Plan against Disinformation' JOIN(2018) 36 final page 9.

[52] About the experimental use of sunset clauses *see* Antonios Kouroutakis, 'The Constitutional Value of Sunset Clauses' (Routledge, 2017); Sofia Ranchordás, *Constitutional Sunsets and Experimental Legislation; A Comparative Perspective* (Edward Elgar, 2014).

[53] Code of Practice against disinformation: Commission calls on signatories to intensify their efforts' (2019) <http://europa.eu/rapid/press-release_IP-19-746_en.htm> accessed 23 June 2019; 'Code of practice against disinformation: Commission takes note of the progress made by online platforms and urges them to step up their efforts' (2019) <http://europa.eu/rapid/press-release_STATEMENT-19-1757_en.htm> accessed 25 June 2019.

[54] EU versus Disinformation, 'Russia is not interfering in the EU elections' (*EU versus Disinfo*, 11 March 2019) <https://euvsdisinfo.eu/report/russia-does-not-interfere-into-the-eu-elections/> accessed 1 May 2019.

Third, the EU Action Plan over relied on self-regulation and self-policing which was not always proven 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'.[55] Although this policy increased the transparency in the social platforms and the awareness of the users about how social platforms use their data, and how they are targeted by advertisements, it seems that this policy missed out significant amounts of crucial information.[56]

Furthermore, the EU Action Plan granted discretion to social platforms to regulate free speech and control public debate. Such platforms for instance have unchecked power to decide the content of free speech, and even to deactivate user profiles. A UN 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'.[57] This declaration encapsulates the general concern about the fine line between free speech and its disproportionate oppression.

Having said that, a more permanent framework would be necessary. Such framework needs to include more specific regulations about the role and the obligations of all social platforms and internet providers.

Conclusions

This article has examined the issue of disinformation. It explored its evolution and remarked the escalation of the problem due to technological advancements. As disinformation affects 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 of May 2019 the EU Commission has adopted and implemented the European Action Plan against disinformation. This Action Plan in reality was a modest regulatory intervention, which was based on soft law and self-regulation.

The action plan was focused on four core areas: first on the improved detection of disinformation, second on the coordinated responses of disinformation, third on the cooperation with online platforms and the industry, and finally on the raising awareness and building resilience amongst citizens. The success of the action plan was based on the cooperation of the public authorities, of the platforms and the people.

Public authorities had mainly a supervisory role. Moreover, they increased the budget with 3.1 million Euros, from 1.9 million euros in 2018 to 5 million Euros in 2019. Furthermore, the Action Plan imposed a set of obligations to social platforms and internet

[55] Code of Practice on Disinformation (n 50).

[56] 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* Privacy International, 'Why Am I seeing this on Facebook? It's still unclear.' (*Privacy International*, 1 April 2019) <https://privacyinternational.org/news/2772/why-am-i-seeing-facebook-its-still-unclear> accessed 1 May 2019.

[57] Organization for Security and Co-operations in Europe and others, 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation And Propaganda' (3 March 2017) <www.osce.org/fom/302796?download=true> accessed 3 May 2019.

providers such as the periodic report and the measures taken on their behalf to prevent and block disinformation incidents and actors. Finally, the Action Plan focused on how public authorities and platforms can raise awareness to 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, as there was no hard law obligations, and finally it was experimental for 12 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 this experience of the Action Plan, a more permanent framework is necessary, as disinformation seems to be an omnipresent threat with more concrete obligations on behalf of the social media platforms and internet providers.