MYKOLAS ROMERIS UNIVERSITY
MYKOLAS ROMERIS SCHOOL OF LAW
INSTITUTE OF INTERNATIONAL AND EUROPEAN UNION LAW

PAULINE LAPOINTE
(EUROPEAN UNION LAW AND GOVERNANCE STUDY PROGRAMME)

EUROPEAN ACTION AGAINST DISINFORMATION: BALANCING FREEDOM OF EXPRESSION WITH NATIONAL SECURITY

Master thesis

Supervisor – Prof. dr. Regina Valutytė

Vilnius, 2019

Table of Contents

LIST OF ABBREVIATIONS **3**

INTRODUCTION **4**

I. DETERMINING THE TERMINOLOGY REFLECTING THE PHENOMENON OF SPREADING FALSE INFORMATION **12**

1. CHARACTERISTICS OF THE PHENOMENON OF SPREADING FALSE INFORMATION 12

1.1. Defining information 12

1.2. The intentions behind the spread of false information 15

1.3. The consequences of the spread of false information 17

2. EXISTING TERMINOLOGY TO DESIGNATE THE DISSEMINATION OF FALSE INFORMATION 18

2.1. Information Warfare 19

2.2. Fake news 19

2.3. Disinformation 20

2.4. Misinformation 21

2.5. Propaganda 21

II. BALANCING INTERESTS: FREEDOM OF EXPRESSION AND NATIONAL SECURITY **24**

1. THE HIGH PROTECTION OF FREEDOM OF EXPRESSION UNDER THE ECHR 24

1.1. The broad scope of freedom of expression 24

1.2. A strict control of the limitations 26

2. THE HETEROGENEOUS REGULATIONS OF THE MEMBER STATES RELATED TO DISINFORMATION 30

2.1. The absence of a common definition of disinformation in national legislations 31

2.2. The lack of common measures to tackle disinformation in national law 33

2.3. The assessment of the compatibility of the national approaches with the ECHR and their efficiency 36

III. THE OPPORTUNITY OF A EUROPEAN UNION ACTION **44**

1. THE EUROPEAN UNION COMPETENCES AND EXISTING REGULATIONS RELATED TO DISINFORMATION 44

1.1. Security and integrity: the external competence of the EU 44

1.2. The shared competence regarding the internal market of the European Union 47

2. THE POTENTIAL DEVELOPMENTS OF A EUROPEAN UNION ACTION 53

2.1. The limits of the self-regulatory approach 53

2.2. Towards a new system of responsibility for the platform providers 57

ABSTRACT **75**

SUMMARY: **76**

LIST OF ABBREVIATIONS

AI: Artificial Intelligence

AVMS: Audio-Visual Media Services

CCBE: Council of Bars and Law Societies of Europe

CSA: Conseil supérieur de l'audiovisuel (French Regulator Council for Audio-visual)

COO: Country of Origin

DDHC: Déclaration des Droits de l'Homme et du Citoyen (French Declaration of Human Rights)

ECJ: European Court of Justice

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

EEAS: European External Action Service

EP: European Parliament

EU: European Union

EU Charter: European Union Charter on Fundamental Rights

GDPR: General Data Protection Regulation

HLEG: High Level Expert Group

ICCPR: International Covenant on Civil and Political Rights

LRTK: Lietuvos radijo ir televizijos komisija (Lithuanian Regulator for Audio-visual)

NetzDG: Network Enforcement Act (Germany)

OSCE: Organization for Security and Co-operation in Europe

PESCO: Permanent Structured Cooperation

RT: Russia Today

TEU: Treaty of the European Union

TFEU: Treaty on the Functioning of the European Union

UDHR: Universal Declaration of Human Rights

UK: United Kingdom

UN: United Nations

US: United States

INTRODUCTION

Between 2015 and 2017, 80.000 Facebook posts were published by Russia-based operatives and seen by 126 million Americans (half of the total population); 2.752 Twitter accounts were found linked to Russian operatives; and Google identify 4,700$ of Russia-linked ad spending in 2016[1]. Those are the numbers revealed, after the American election of 2016, during the hearing of the executives from Facebook, Twitter and Google before three United States (US) congressional committees[2]. The outcomes of the American elections are known but the extent of the Russian influence remains difficult to quantify. Was Donald Trump victory due to Russia involvement or did the democratic process remain intact even if a major disinformation campaign was organised by a foreign State? The question here is the consequence and impact of false information in the functioning of the State society, including its democratic process, but also social cohesion, trust, health, economy, etc.

The phenomenon of spreading false information is not new, the Experts dated it back to 480 BC and Themistocles spreading false information on the Persian army[3]. Another example took place in the end of the 19th century, in France, where, the aggregation of false information, public opinion and antisemitism led to the condemnation for treason of an innocent French soldier: the unfortunately famous Dreyfus Case[4]. Finally, during the 20th century, war and confrontation of societies' ideology conducted states to engage in propaganda in different scales[5]. However, at the end of the cold war, most of researchers shifted away propaganda, thinking that it was, from now on, an old phenomenon: what Florian Zollman named "The Marginalisation of Propaganda"[6].

---

[1] Reuters. David Ingram, "Facebook says 126 million Americans may have seen Russia-linked political posts", October 31 2017,
https://www.reuters.com/article/us-usa-trump-russia-socialmedia/facebook-says-126-million-americans-may-have-seen-russia-linked-political-posts-idUSKBN1CZ2OI

And: Free Speech and the Regulation of Social Media Content, Congressional Research Service, March 27, 2019, https://fas.org/sgp/crs/misc/R45650.pdf

[2] Ibid

[3] "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States", European Parliament Report, February 2019,

https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

[4] Ministère de la Justice, « L'affaire Dreyfus », 23 August 2011: http://www.justice.gouv.fr/histoire-et-patrimoine-10050/proces-historiques-10411/laffaire-dreyfus-22696.html

[5] "Bringing Propaganda Back into News Media Studies", Florian Zollmann Newcastle University, UK, Critical Sociology 2019, Vol. 45(3) 329 –345, DOI: 10.1177/0896920517731134 journals.sagepub.com/home/crs

[6] Ibid

However, the phenomenon of spreading false information, in order to manipulate populations, took recently a new extent and resurrected the interest on this matter. The terminology has changed, as it is now commonly designed as fake news. The Cambridge Dictionary even consecrated it as the word of the year in 2017. Even if the substance of the phenomenon (spreading false or misleading information to influence public opinion) is the same, the extent of it is far more alarming. The new means to distribute false information are global, direct and without regulations. The social medias, such as Facebook, Twitter, Instagram, but also private messages apps like WhatsApp or Snapchat, provide citizens with possibility to access directly a variety of information without any institutionalised pre-filter[7]. Moreover, the form of the information has changed. In 1966, Arthur Larson expressed his concerns about the development of television when he could see the effect of propaganda on radio, which he qualified as a swift mode of communication with a potential to "reach people whether literate or illiterate" and its emotional influence through "the timbre and expression of the human voice". Finally, he emphasized the "extreme difficulty of combating or blocking it"[8]. It sounds familiar with how Internet and social media are described, but with an exponential development of what the radio could do: today, people have the information in their hands. Anyone with education or not, without age restriction can access the information and can create it. Governments cannot block it - exception of measures affiliated to censor - and, it is not only just a voice, it is images, live videos, expressions, reactions, symbols that are used. Finally, the techniques used by the authors of false information are much more advanced with the use of Artificial Intelligence (AI), bots, trolls, etc. and allow a dissemination in a scale never reachable before.

The consequences of false information are hard to quantify and ascertain. Did targeted ads and Russian driven Facebook profiles determined the outcome of the American elections of 2016? Did the 261 media articles of Russia Today (RT) and Sputnik and the "156,252 Russian accounts tweeting about Brexit"[9] swing the British votes to the leaving option in 2016? To which extent the "Macron leaks" and the rumours spread by Russian sources influenced the French Presidential elections of 2017? Did the 100 000 accounts banned by WhatsApp influenced Brazilian voters in favour of the populist Jair Bolsonaro? The phenomenon of providing false information can affect a variety of domains such as the health, with false information campaign

[7] Ibid

[8] "The Present Status of Propaganda in International Law", Arthur Larson, Law and Contemporary Problems, Vol. 31, No. 3, International Control of Propaganda (Summer, 1966), pp. 439-451, Published by: Duke University School of Law, Stable URL: https://www.jstor.org/stable/1190732

[9] "Disinformation and 'fake news': Interim Report Contents, "Russian influence in political campaigns" https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm#_idTextAnchor033

regarding vaccination[10], trust in military with, for example, false information campaign against NATO Soldier in Lithuania[11]. It affects all the spheres of society and even if it is easy to find an influence of false information on those events, States are not measuring yet the consequences and are still lacking a strong will to regulate the phenomenon: unclear terminology, lack of efficient responsibility regimes, etc. After the results of the American elections, experts and governments realised the necessity to understand this phenomenon. The Senate of the United-States (US) started to have hearings to understand better the extent of the phenomenon. The United Kingdom (UK) did the same after the Brexit referendum. French President Emmanuel Macron declared, soon after its election, his intention to have a law to protect the elections process, which was adopted in 2018[12]. The European Union (EU) also emphasizes the importance to respond to false information. Firstly in communication of the European Commission (e.g. Communication on Tackling online disinformation of 2018[13]), then by actions such as the Action Plan against Disinformation and the Code of Good practice[14] and finally the European Parliament (EP) concerned for the security of the elections of 2019 also conducted research in this field[15] and took a Resolution in October 2019 regarding foreign electoral interference[16].

The first attempt of the researchers was to define the phenomenon of spreading false information online, in order to influence public opinion. The High Level Expert Group (HLEG) Report excludes the term fake news and prefers the term disinformation. Most of the research consecrate the same analysis to exclude fake news as there is a "notable lack of consistency among human rights organisations using the term 'fake news'" and because of its ambiguous

---

[10] World Health Organisation. "Vaccine misinformation: statement by WHO Director-General on Facebook and Instagram", 4 September 2019, Geneva: https://www.who.int/news-room/detail/04-09-2019-vaccine-misinformation-statement-by-who-director-general-on-facebook-and-instagram

[11] LRT. "More fake news target NATO's presence in Lithuania", 2019-09-27: https://www.lrt.lt/en/news-in-english/19/1101632/more-fake-news-target-nato-s-presence-in-lithuania

[12] Law n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id

[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling online disinformation: a European Approach*, Brussels, 26/04/2018, EUR-LEX : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

[14] "EU Code of Practice on Disinformation", European Commission, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[15] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, Report requested by LIBE Committee: http://www.europarl.europa.eu/supporting-analyses

[16] European Parliament resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP))

character[17]. However, there is no consensus on the proper term to use. Some are using disinformation, other misinformation, mal-information, information warfare, or finally propaganda. Moreover, when discussing the definition and the appropriate terminology, few authors are taking the approach chosen here, meaning, starting from a complete description of the phenomenon to emphasize its characteristics before analysing the existing terms. The objective is to have a complete understanding of the phenomenon before analysing the terms related and the one(s) fitting best.

The spread of information, true or false, is undeniably linked to the fundamental right of freedom of expression. Freedom of expression includes not only the right to free speech, express opinions and ideas, but also the right to receive and impart information. This right is one of the most incontestable rights for democratic society as the basis for "political debate, truth finding, social cohesion, avoidance of censorship and self-development"[18]. It is consecrated in most International legal instruments such as Article 19 of the Universal Declaration of Human Rights (UDHR)[19] and of the International Covenant on Civil and Political Rights (ICCPR)[20], Article 10 of the European Convention on Human Rights (ECHR)[21] and Article 11 of the European Union Charter of Fundamental Rights (EU Charter)[22]. It is also found in national constitutions: Article 11 of the Déclaration des Droits de l'Homme et du Citoyen (DDHC - France)[23], Article 25 of the Lithuanian Constitution[24], etc. Freedom of expression is not limited to the ideas that comply with the State perspective, it includes also the ones that "offend, shock or disturb the State or any sector of the population"[25]. The European Court of Human Rights (ECtHR) justified this broad interpretation of freedom of expression on the ground of pluralism, tolerance and broad mindedness, which constitute the basis of a "democratic society"[26]. However, some state security institutions alert that the purveyors of false information usually use freedom of expression and a

[17] Ibid

[18] Sarah Eskens, Natali Helberger & Judith Moeller (2017) Challenged by news personalisation: five perspectives on the right to receive information, Journal of Media Law, 9:2, 259-284, DOI: 10.1080/17577632.2017.1387353

[19] Universal Declaration of Human rights, 1948: https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf

[20] International Covenant on Civil and Political Rights, 1966 : https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

[21] European Convention on Human Rights, 1950: https://www.echr.coe.int/Documents/Convention_ENG.pdf

[22] EU Charter of Fundamental Rights, 2000: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[23] Déclaration des Droits de l'Homme et du Citoyen, 1789: https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789

[24] Lithuanian Constitution, 1992: https://www.lrs.lt/home/Konstitucija/Constitution.htm

[25] ECHR, Handyside v. the United Kingdom, judgment of 7 December 1976, §49.

[26] Ibid

biased interpretation of it, for brandishing the censorship alerts in order to avoid any regulation or actions to tackle the intentional spread of false information[27]. Nevertheless, some limits of this right have always been accepted in order to have a balanced system of protection of the fundamental rights. In this regard, hate speech, defamation and incentive to violence are generally prohibited (Article 19 ICCPR), and most of States consider it as a crime or offence. However, there is no consensus regarding the prohibition of spreading false information, which conducts to asymmetries in the European legislations and the national protection of speech. It is not per se an issue to have different national acceptation of the limitation of fundamental rights, as long as those limitations remain an exception and are answering a triple test condition: the limitations must have been prescribed by the law[28], they have to be necessary for the protection of the democratic society[29] and proportionate in regard of the goal of general interest[30] (Article 10(2) ECHR). Indeed, States benefit from a certain margin of appreciation depending on the protected interest. Regarding the spread of false information by a foreign State it is usually related to the principle of State security and territorial integrity (Article 2(4) UN Charter). Indeed, the phenomenon can endanger the democratic process and institutions of a State or as the Ukrainian case and the annexation of Crimea illustrates, it can have consequences on the territorial integrity of a State[31]. When States apply national security or territorial integrity objectives, they usually enjoy a wide margin of appreciation, and the ECtHR restricts its control. Freedom of expression in itself benefits from a large amount of research papers and both the ECtHR and the ECJ have detailed reports on their case law for a better understanding[32]. However, for now, the case law is mostly related to illegal speeches such as hate speech, or defamation[33]. Therefore, the consequences of propaganda on State integrity have been analysed[34] but few researches have been conducted regarding the balance and compatibility, with freedom

---

[27] National Threat Assessment 2019, State Security Department of the Republic of Lithuania, Vilnius 2019

[28] ECHR, Herczegfalvy v. Austria, judgment of 24 September 1992 §93 and 94.

[29] ECHR, Autronic AG v. Switzerland, judgment of 22 May 1990, §61 : "The necessity for restricting them must be convincingly established

[30] ECHR, Thorgeir Thorgeirson v. Iceland, judgment of 25 June 1992

[31] How to Stop Disinformation Lessons from Ukraine for the Wider World, by Marina Pesenti and Peter Pomerantsev, Transitions Forum, Beyond Propaganda | August 2016

[32] Freedom of expression in Europe, Case-law concerning Article 10 of the European Convention on Human Rights, available here: https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-18(2007).pdf

[33] ECHR Factsheet – Hate speech, October 2019

[34] "International Propaganda and Minimum World Public Order", William V. O'Brien, Law and Contemporary Problems, Vol. 31, No. 3, International Control of Propaganda (Summer, 1966), pp. 589-600. Stable URL: https://www.jstor.org/stable/1190741

of expression, of blocking foreign contents in order to limit the dissemination of false information, as endangering State security.

Secondly, scholars usually limit their analysis to the European legal order, or to one Member State's regulations in relation to the EU. Indeed, at the national level, as soon as France adopted the "anti-fake news Law" scholars analysed its efficiency and the limitations regarding freedom of expression[35], same for Germany and the "Network Enforcement Act" (NetzDG) [36]. At the EU level, the main preoccupation was the elections of the EP of 2019, and the discussion of the competence of the EU and its margin of action. In addition, since 2018, as the European Commission adopted a Code of Good Practice, which is a code of self-regulation for the relevant and engaged stakeholders, the research analysed the adequacy and suitability of a self-regulatory approach[37]. The opinions are usually divided on this matter. On one hand, for example, Boris Barraud[38] considers that the platforms are driven by economic purposes, which render auto-regulation inefficient. On the other hand, some recognised auto-regulation only as a first step, which should be complemented by regulations[39]. Here, a comparative analysis of the initiatives in three Member States (France, Germany and Lithuania) will be conducted before examining the opportunity and the necessity of a EU approach.

[35] See for example : « Analyse juridique de la proposition de loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information », Commissioned by the Office of the OSCE Representative on Freedom of the Media from Laurence Franceschini, Independent Media Freedom Expert, November 2018. Le Lamy droit des médias et de la communication, 218-4 - Nouvelles technologies et qualité de l'information. « Fake news, infox, quelles réponses juridiques ? » Myriam Quéméner, Magistrat - Docteur en droit, Dalloz IP/IT 2019 p.178

[36] See for example: "How to Counter Fake News? A taxonomy of anti-fake news approaches", by Alberto Alemanno. « Fake news : une loi polémique, qui pose plus de questions qu'elle n'en résout », Constitutions 2018 p.559, Diane de Bellescize, Professeur émérite de l'Université du Havre

[37] See for example: Avis du Comité économique et social européen relatif à la communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions Plan d'action contre la désinformation [JOIN(2018) 36 final], JOUE (C) 5 Juillet 2019. The Tallinn Guidelines on National Minorities and the Media in the Digital Age & Explanatory Note February 2019 OSCE HCNM. On Regulating International Propaganda: A Plea for Moderate Aims, Richard A. Falk, Source: Law and Contemporary Problems, Vol. 31, No. 3, International Control of Propaganda (Summer, 1966), pp. 622-634, Published by: Duke University School of Law, Stable URL: https://www.jstor.org/stable/1190743, Accessed: 08-11-2019 17:25 UTC

[38] « La lutte contre les fausses informations sur internet : un jeu de lois », Boris BARRAUD (Docteur en droit), Revue Lamy Droit de l'Immatériel, Nº 154, 1er décembre 2018

[39] See for example : Rapport d'information déposé par la Commission des affaires européennes, portant observations sur les proposition de loi organique et proposition de loi relatives à la lutte contre les fausses informations (nos 772 et 799), M. Pieyre-Alexandre ANGLADE, Député. L'analyse juridique de la proposition de loi française relative à la Lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information, Commissioned by the Office of the OSCE Representative on Freedom of the Media from Laurence Franceschini, Independent Media Freedom Expert. Avis du Comité économique et social européen relatif à la communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions Plan d'action contre la désinformation [JOIN(2018) 36 final], JOUE (C) 5 Juillet 2019. Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, Report requested by LIBE Committee: http://www.europarl.europa.eu/supporting-analyses

Aim of the Research:

This research aims at analysing the best ways for the EU to tackle the phenomenon of spreading false information, in respect of the fundamental rights, by defining it and emphasizing the absence of a uniform approach of the different legislation of the Member States, leaving the place for the EU to step in.

Objectives of the Research:

For achieving this aim, the following objectives are set:

1. To disclose the content of the characteristics of the spread of false information by comparing different terminologies and determining the best terminology to reflect properly the phenomenon in order to propose an harmonisation of the terminology at the EU level.

2. To elaborate if the Member States have the opportunity, and to which extent, to use the principle of State integrity to block foreign content disseminating false information, as defined in the first part, while respecting freedom of expression, enshrines in the EU Charter and the ECHR, by conducting an analysis of the relevant case law of the ECtHR.

3. To disclose the possibility and opportunity of a EU approach by analysing whether the national initiatives in selected Member States are uniform and efficient enough.

Research Methodology:

For achieving the aim and objectives, the terminological analysis and description methods permitted to conceptualize the phenomenon of the dissemination of false information. Indeed, starting from the description of the phenomenon of dissemination of false information, it permitted to reveal the main characteristics and have a complete understanding of the different aspects. This descriptive methods, combined with the analysis of the existing terminology revealed the nuances and specificities of the phenomenon to tackle.

The comparative method and the legislative analysis used regarding the legislation of the national states are particularly relevant to emphasize the lack of a uniform approach from the Member States. Indeed, only by comparing the existing legislations of the Member States it is possible to demonstrate the lack of uniformity inside the EU, as well as the arising issues regarding the efficiency of such separate approaches.

Finally, the analytical method was used regarding the EU competences and its possibility to step in. The principle of conferral competences limits the EU domains of actions to the one enshrine in the treaties. In the context of false information, the EU can invoke two

competences. Firstly, the shared competences as it affects the internal market, and secondly the external competences of the EU as the dissemination of false information can endanger the security and territorial integrity of the EU. The analysis of the current Directives related to Internet and Media service providers demonstrate the existence of the exercise of EU competence in this matter, and can serve as a basis for further actions, especially regarding an harmonisation of the status of the platform providers and their obligations.

Structure of the research:

After this introduction, the research is structured with a first part dedicated to the understanding of the characteristics of the phenomenon of spreading false information in order to determine the best terminology to use. The second part focuses the analysis on the necessary balance between freedom of expression and state security for the national states when regulating the dissemination of false information. Finally, the third part analyses the scope of the EU competences and possibilities of actions regarding the dissemination of false information, as the approach of the national states might be insufficient.

Defence Statement:

The EU should establish a common framework regarding the definition and responsibility of the platform providers in order to tackle efficiently the dissemination of intended false information, as the national approaches are insufficient and may impair the digital single market.

I. DETERMINING THE TERMINOLOGY REFLECTING THE PHENOMENON OF SPREADING FALSE INFORMATION

The term "fake news" became worldwide known after the 2016 American elections, but designed an imprecise phenomenon. As was mentioned above there are number of different terms used to describe the phenomenon, thus the first sub-part will analyse the phenomenon of spreading false information in all its aspects to reveal its characteristics (1) before analysing the different existing terms and determining the best terminology to reflect the phenomenon (2).

1. Characteristics of the phenomenon of spreading false information

The starting point, in understanding this phenomenon is the delimitation of the definition of an information (1.1), before determining the intention (1.2) and to finally analyse the consequences of the phenomenon on the individuals and on society (1.3).

1.1. Defining information

The definition of an information is a pre-requisite when analysing the phenomenon of "fake news". The International Code of Journalistic Ethics of 1983, in its Principle II, called "The journalist's dedication to objective reality"[40], defines the task of a journalist as to "serve the people's right to true and authentic information, through an honest dedication to objective reality, whereby facts are reported conscientiously". The Resolution 1003 of 1993 of the Parliamentary Assembly of the Council of Europe emphasizes that "a clear distinction must be drawn between news and opinions. News is information about facts and data, while opinions convey thoughts, ideas, beliefs or value judgments" (Point 3)[41]. Point 21 alerts on the necessity for journalists not to "alter truthful, impartial information or honest opinions, or exploit them for media purposes, in an attempt to create or shape public opinion". Finally, Point 36 reaffirms the "fundamental right of the citizens to receive truthful information and honest opinions". The term "information"

---

[40] International Code of Journalistic Ethics of 1983, Principle II: "The journalist's dedication to objective reality": The foremost task of the journalist is to serve the people's right to true and authentic information through an honest dedication to objective reality whereby facts are reported conscientiously in their proper context, pointing out their essential connections and without causing distortions, with due deployment of the creative capacity of the journalist, so that the public is provided with adequate material to facilitate the formation of an accurate and comprehensive picture of the world in which the origin, nature and essence of events, processes and states of affairs are understood as objectively as possible.
https://accountablejournalism.org/ethics-codes/International-Principles

[41] Resolution 1003 (1993), Ethics of journalism, Parliamentary Assembly, Council of Europe.
https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16414&lang=en

is associated with the adjectives “authentic”, “objective reality”, “truthful, impartial” and the “facts and data”. In this regard, the information must be based on a reality, a fact, admissible for all individuals and not relying on an interpretation or an opinion. In this respect Boris Barraud identifies three criteria to define information: i) it has to be related to a fact; ii) the knowledge of the fact must represent an interest for the public (flexible notion); and iii) the reality of the fact must be verifiable and certain[42].

1.1.1. The existence of verifiable facts and data

The false information by definition is not information, and therefore should be excluded from the definition of an information and of the scope of the Article 10 of the ECHR. A false information is neither an opinion nor an idea. Boris Barraud defines it as “a statement presented as a fact, an event, which did not take place, or at least whose reality cannot be verified […] a false information is a non-information”[43]. However, it might be very difficult to distinguish information from an opinion or a false information or satire and parody. Indeed, the information as the result of a transmission is never just about the fact: it is also an interpretation of the fact or reality, indicating personal choices and values. Therefore, the truthfulness of an information, according to Boris Barraud, is more measured according to the method employed to deliver it: did the author have an idea and looked for a proof to support his idea or on the contrary, did he encounter a fact and then provide an explanation[44]. Another, even more insidious technique exists: the information is true but only selected facts or elements are transmitted from which results complete bias information leading to a misunderstanding of the situation. This technique goes against the Code of ethics of Journalism and the Journalist’s dedication to objective reality and reporting the fact conscientiously.

The false information might be followed by the intention of the author or by genuine believe that the information is true. Some try to influence the opinion to harm or make profits, or to diffuse the author ideology (see below point 1.2). But some false information can exist also by error of the author or on the contrary in the intention to entertain the public such as parody. The danger is not coming from the parody, which might be provocative (e.g. Charlie Hebdo cover-page parodying Mahomet) but the authors’ intention is either to entertain or to encourage

[42] « La lutte contre les fausses informations sur internet: un jeu de lois », Boris Barraud, Revue Lamy Droit de l'Immatériel, n°154, 1er Décembre 2018.

[43] Ibid

[44] Ibid

thinking and public debate among the public opinion. The ECtHR consider it as a “form of artistic expression”[45].

1.1.2. The exclusion of some type of speeches from an information

The ECHR and the EU Charter include in the freedom of expression not only the right to receive and impart information but also the right to hold opinions and ideas. The opinions and ideas must be distinguished from the information: it is commonly accepted to exclude them and rumors from the definition of an information.

Nevertheless, the distinction between information and opinion is not always easy to disclose: when giving information, journalists can express their opinions, which are mixed with the content of the information. The expression of opinions is well protected by the ECtHR especially when it concerns political debate[46]. E.g. in *Lopes Gomes da Silva v. Portugal*, 28 September 2000, the ECtHR stated that freedom of expression was not limited to ideas that are favorable to the State, it included also the ones that “offend, shock or disturb the State or any sector of the population”. The ECtHR justified it on the ground of pluralism, tolerance and broadmindedness, which constitute the basis of a “democratic society”[47]. Only a significant abuse can be subject to limitation of the freedom of expression of the press[48].

Finally, some illegal contents are excluded from the definition of information and of the protection offered by the freedom of expression such as hate speech, incitement to violence and defamation[49]. Indeed “tolerance and respect for the equal dignity of all human beings constitute the foundations of a democratic, pluralistic society […] it may be considered necessary to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred”[50].

To sum up, the information, protected under the fundamental right of freedom of expression, can be defined as based on real, verifiable and objectives facts. The false information by opposition is not information because it is not based on an objective presentation of the fact, either because the fact is not real or verifiable, or because the presentation of the fact is

[45] ECHR, Ziembiński v. Poland (No. 2), (Application no. 1799/07), 5 July 2016

[46] ECHR, Lopes Gomes da Silva v. Portugal, No. 37698/97, judgment of 28 September 2000, Reports 2000-X, §34

[47] ECHR, Handyside v. the United Kingdom, judgment of 7 December 1976, Series A No. 24, §49.

[48] ECHR, Prager and Oberschlick v. Austria judgment of 26 April 1995, Series A no. 313, pp. 17-18, paras. 34-35

[49] Article 20 ICCPR

[50] ECHR, Erbakan v. Turquie, No 59405/00, 6 juillet 2006.

subjective and bias, conducting to a misunderstanding of the situation. The opinions or ideas (also protected by the freedom of expression), the satire and parody, and finally illegal content such as hate speech and defamation are excluded from the definition of information. However, it has to be bear in mind that it is difficult to draw a strict separation between information and opinions as, the authors usually reflect their opinions when presenting information.

1.2. The intentions behind the spread of false information

1.2.1. Political destabilization

States are one of the main sources of false information. A foreign state can benefit from destabilisation of the other States and can use it to affirm its primacy or at least legitimacy. For example, the EU and the US[51] have clearly identified Russia as one of the main foreign sources of such content. The impact of the false information on the American elections or on the United-Kingdom has resulted in a weaker "western" position, benefiting to other States. The diffusion of massive false information in Ukraine led to the annexation of Crimea and major tensions in the rest of Ukraine, favouring Russia's influence over the region[52]. However, the exact assessment of the scope of such interference and its consequences remain today difficult to ascertain by lack of research[53].

In the case of national State spreading false information, States can also benefit from a divided society to maintain their power. Usually it concerns non-democratic states or the one flirting with the respect of human rights that can benefit from false information in order to maintain a control on the society. In this case, spreading false information goes usually in hand with censorship. Some concerns have been raised inside the EU, notably regarding Hungary with the Government funding disinformation campaigns[54].

---

[51] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: a European Approach, 26 April 2018

And Report of the Select committee on intelligence United States Senate on "Russian active measures campaigns and interference in the 2016 U.S. election, Volume 2: Russia's use of social media with additional views https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[52] Foreign Affairs, "Why Putin took Crimea – The Gambler in the Kremlin" by Daniel Treisman, May/June 2016, https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-russian-president-putin-took-crimea-from-ukraine

[53] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019

[54] Ibid, "1.3.3.1 Hungarian government campaigns against migrants and against George Soros", p44

1.2.2. Economical interest

Sometimes linked to political destabilization, the false information can benefit economically to different actors. First regarding the State, it can be illustrate with the example of Russia gaining influence in Ukraine, which represents an important market for Russia[55]. But companies or economic groups can also be the source of false information, usually to serve their private economic interest. Lobbying, to a certain extent, can be sources of spreading false or at least misleading information as for example during the campaign regarding the Copyright Directive[56]. The health sector is also impacted in a large scale with false information regarding vaccination[57].

Medias also can be the source of false information. In regard of the self-regulation existing, false information produced by media might be either an error, or the sign of poor quality journalism[58]. However, as false information is usually more attractive than real one, modern journalism, especially online, can have major gain with false information, or at least misleading headlines in order to get revenue from the number of clicks or views[59]. This is the phenomenon of clickbait: putting emotional, misleading headlines in order to have people clicking or sharing it to gain more revenue from publicity sector[60].

Finally, citizens are also sometimes sources of spreading false information as a profitable business. For example, investigation revealed that some Macedonians citizen employed to publish false information, were earning three times the average wages[61].

---

[55] World Finance – The Voice of the Market, "Crimea doesn't pay: assessing the economic impact of Russia's annexation", Barclay Ballard, October 28 2019: https://www.worldfinance.com/strategy/crimea-doesnt-pay-assessing-the-economic-impact-of-russias-annexation

[56] European Parliament News, "Questions and Answers on issues about the digital copyright directive", Press Releases, 27-03-2019: https://www.europarl.europa.eu/news/en/press-room/20190111IPR23225/questions-and-answers-on-issues-about-the-digital-copyright-directive

[57] World Health Organisation. "Vaccine misinformation: statement by WHO Director-General on Facebook and Instagram", 4 September 2019, Geneva: https://www.who.int/news-room/detail/04-09-2019-vaccine-misinformation-statement-by-who-director-general-on-facebook-and-instagram

[58] Journalism, fake news & disinformation: handbook for journalism education and training, UNESCO, Ireton, Cherilyn, Posetti, Julie, 2018, ISBN:978-92-3-100281-6 https://unesdoc.unesco.org/ark:/48223/pf0000265552

[59] Adperfect, "How fake news is creating profits", October 26, 2017: https://www.adperfect.com/how-fake-news-is-creating-profits/

[60] BBC, "Clickbait: The changing face of online journalism", Ben Frampton, 14 September 2015, https://www.bbc.com/news/uk-wales-34213693

[61] "She was paid 3 euros per post, amounting to a mere 24 euros per day. That's not much to some, but triple what she might have earned doing a job locally". BBC, "I was a Macedonian fake news writer", Simon Oxenham, 9th May 2019: https://www.bbc.com/future/article/20190528-i-was-a-macedonian-fake-news-writer

1.3. The consequences of the spread of false information

1.3.1. The consequences on individuals

False information affects firstly the individuals. When receiving a false information, the individual may believe it as true, it may have a critical look, or it may spot the false information and then lose trust in the source of information. False information affects in general the trust in the media and the information[62]. It affects the individual's right to receive information, protected by the article 10 of the ECHR and Article 11 of EU charter. Freedom of expression is based on different ideals, which are the ability for a citizen to develop its own thinking and critical knowledge, the quest of truth, and, in a global perspective, the way for the citizen to make a thoughtful vote during the democratic process. The dissemination of false information hinders those rights.

False information impacts another fundamental right of the citizen, which is the right of data privacy. In the European legal order, data privacy is related to the right to a private life (Article 8 ECHR) whereas in the EU, the article 8 of the EU Charter specifically concerns the right to the protection of personal data. How is the spread of false information related to data privacy? It has been revealed, specifically with the Cambridge Analytica scandal, that data of the citizens were used against them in order to target them with specific content[63]. Publicity bought by different actors (politics, companies) is targeting users according to their sex, age, nationality, interests, etc. And with Cambridge Analytica, it appears that those data have been illegally used in order to target different social groups and encourage them to vote in one way or another[64]. Therefore, two distinct issues are arising from the false information and the data privacy. First, data of citizens have been collected and used for ends they were not aware of, which is a breach of their rights for privacy. Secondly, it has been used to target and manipulate them, which is against their free determination, and will: it affects their dignity[65].

---

[62] EP Report 2019: "When no distinction was made in the questionnaire between online and offline media, the results were significantly lower: only 34 % trusted "the media" and 61 % did not trust it"

[63] European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP))

[64] The Guardian, "Facebook faces fresh questions over when it knew of data harvesting", Carole Cadwalladr, 17/03/2019, https://www.theguardian.com/technology/2019/mar/16/facebook-fresh-questions-data-harvesting-cambridge-analytica

[65] "The act of micro-targeting based on sensitive information violates human dignity, the right to freedom of (truthful) information and distorts public discourse", European Parliament Report, p131.

1.3.2. The consequences on society

The example of the American election or the Brexit proves that spreading false information affects the democratic process. Described as "the triangular relationship between the Fundamental Rights, Democracy and the Rule of Law"[66], none can exist without the others. Consequently, when the spread of false information affects fundamental rights of the individuals, especially freedom of expression, it affects the democracy and the rule of law. If the citizen cannot make an informed choice when voting, if it has been misled by false information, then the process of voting loses its value and sincerity. A third party impacts the results of the election.

The second major consequence on the society is its destabilization. Indeed, false information can be spotted which lead usually to a loss of confidence from the citizen toward the media or the authorities. The Eurobarometer indicated an average trust in the media of 50% in 2016 (depending on the source of the media: the radio as the most trust media and social media as the less trustworthy)[67]. Moreover, according to Rob Procter, the objectives of spreading false information is not much about making people believe in it but to make them doubting about the truthfulness of any information, which leads to distrust[68]. Finally, from this mistrust, in the media and authority, results a general suspicion and more generally a destabilization of the society equilibrium. In addition, this destabilization can be encouraged by spreading even more false information. For example, during the yellow vest jacket movement in France, false information in both sides were used to inflame the opposition[69].

2. Existing terminology to designate the dissemination of false information

Multiple terms exist in order to speak about false information. The multiplication of terms leads to major misunderstanding in the distinction of the different meanings of each terms. In this section, each terms will be analyzed in order to determine if they fit the characteristics previously developed to finally have a better understanding of which terms to use.

---

[66] Carrera, S, Guild, E & Hernanz, N 2013, 'The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU, Towards an EU Copenhagen Mechanism', Study, CEPS, Brussels

[67] Standard Eurobarometer 88, Autumn 2017, Media use in the European Union, Survey requested and co-ordinated by the European Commission, Directorate-General for Communication.

[68] The Economist, "Disinformation, Lithuanians are using software to fight back against fake news", Martina Paukova, 24th October 2019 https://www.economist.com/science-and-technology/2019/10/24/lithuanians-are-using-software-to-fight-back-against-fake-news

[69] Euractiv, « Les Gilets jaunes noyés sous les infox sur Facebook », Marion Candau, 13/03/2019, https://www.euractiv.fr/section/elections/news/les-gilets-jaunes-noyes-dans-les-infox-sur-facebook/

2.1. Information Warfare

Before the XXI Century, false information was known and used only in the military spheres. Spreading false information with the intention to mislead individuals or cause harm can still be part of information warfare, understood in the wider context of the hybrid threats, designing a huge variety of threats in different fields (diplomatic, military, economic, and technological)[70]. The European External Action Service (EEAS) defines it as a combination of "conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives". This term reflects the potential harm on the democratic institutions and the use of the dissemination of false information as a weapon in a context of destabilisation of the foreign States. However, the problem arising with the term information warfare is its limitation to the military's activity, whereas today, the spread of false information may have other objectives or sources such as economical ones. Moreover, false information is no longer only the product of States or military actors, every citizen can be the source of it. Therefore, this term will be excluded in the following developments because of its restriction to the military sphere.

2.2. Fake news

The term fake news has been widely popularised by its use by well-known politicians – Donald Trump as the first one. The important use of this term permitted to bring the light on the on-going phenomenon. However, by being used by so many politician and citizens all over the world, it loses some scientific precision in its definition and can design too many different things. Thus, the High Level Expert Group (HLEG) Report design fake news as associated "with partisan political debate and poor journalism broadly rather than more pernicious and precisely defined forms of disinformation"[71]. A Report of the UK Parliament of July 2018 also rejects the term fake news because it "has been used to describe content that a reader might dislike or disagree with". Both of those reports recommend the decision-maker to prefer the term disinformation instead of fake news. In comparison with the French terminology, the Commission of enrichment of the French language advises to use the term "infox" (from Information and intoxication) as the French version of "Fake news". Nevertheless, in the Report of the French National Assembly, they prefer to use the term "Fausses informations" literally

---

[70] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation, Brussels, 5/12/2018.

[71] "A multi-dimensional approach to disinformation", Report of the independent High level Group on fake news and online disinformation.

“False information” for the same reasons mentioned above. The term “fake news”, not precise enough and lacking scientific rigor, leads to designate also news with which people simply disagree with[72]. Therefore, the term should be avoided in scientific research and regulations, except if it provides, first, clear delimitation of the understanding of the term.

2.3. Disinformation

By rejecting the term fake news, most of the experts turn to the term “disinformation” which is defined according to the HLEG as: “false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. The risk of harm includes threats to democratic political processes and values, which can specifically target a variety of sectors, such as health, science, education, finance and more. It is driven by the production and promotion of disinformation for economic gains or for political or ideological goals, but can be exacerbated by how different audiences and communities receive, engage, and amplify disinformation”[73]. This definition is quite similar in the Code of Good Practice, which defines it as “verifiably false or misleading information". It has to present two cumulative criteria: the motivation should be the “economic gain or to intentionally deceive the public" and the consequences of this information is the “public harm", understood as "threats to democratic political and policymaking processes” and threats to public interest (health, security, etc.)[74]. The term fits the characteristics developed in the first part, which is logical, as the term has been developed to designate this specific phenomenon. However, by designing this specific phenomenon, the term might be too limited to future unforeseeable development of the phenomenon, which might gain other characteristics. For example, the phenomenon of deep fakes, designating false content which falsification is “to become unrecognisable by both human and machine control”, will soon present new challenge as the falsity will be unrecognisable[75].

---

[72] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019

[73] “A multi-dimensional approach to disinformation”, Report of the independent High level Group on fake news and online disinformation.

[74] “EU Code of Practice on Disinformation”, European Commission, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[75] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019, Point 5.1.2

2.4. *Misinformation*

The prefix "mis-" is defined as expressing that an action has been done wrongly or badly[76]. The HLEG Report defines misinformation as "misleading or inaccurate information shared by people who do not recognize it as such". The Full-fact report on tackling misinformation in an open society distinguish misinformation which is "the inadvertent spread of false or misleading information; and disinformation [which] is the deliberate use of false or misleading information to deceive audiences"[77]. Misinformation usually designates false information, which are not perceived as such and shared without the intention of sharing false information. The elements are the same, the consequences can be the same as for disinformation but there is no intention of harm or economic interest. The distinction would be relevant regarding responsibility regimes of the authors if such regimes existed. Therefore, according to the context and the elements set forward (intention or not), mis- and dis- information can be used concomitantly.

2.5. *Propaganda*

Propaganda is often used at the same time as disinformation. EP Report of 2019 defines it as "the art of influencing, manipulating, controlling, promoting, changing, inducing, or securing the acceptance of opinions, attitudes, action, or behavior"[78]. In this regard, disinformation and propaganda overlap: information distributed in the intention of influencing people's opinion for political purpose match both definitions. The Joint Declaration on Freedom of Expression and "Fake news", Disinformation and Propaganda of the 3rd March 2017[79] uses the terms Disinformation and Propaganda in a similar perspective. The only distinction made between the two terms can be found in Point 2.6: "State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate reckless disregard for verifiable information (propaganda)." The distinction is a thin one as in both cases, either the person knows or should know it is false information and still disseminates it, or the person is indifferent if the information are true or false in general and disseminates it. In both cases, the person

---

[76] Cambridge dictionary, "mis-": https://dictionary.cambridge.org/dictionary/english/mis

[77] "Tackling Misinformation in an Open Society: How to respond to misinformation and disinformation when the cure risks being worse than the disease", Full-Fact Paper (UK) – 2018

[78] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, Report requested by LIBE Committee: http://www.europarl.europa.eu/supporting-analyses

[79] OSCE, Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, https://www.osce.org/fom/302796?download=true

demonstrates a disregard for truthful information, which justifies the concomitant use of the terms.

However, a distinction should be made with War propaganda, which is prohibited by the Article 20 of the ICCPR[80], and designates propaganda campaigns promoting war or incitement to war, which enters into the meaning of the term information warfare. The phenomenon of false information is a more pernicious way of propaganda used in democratic society, outside a war context, to influence citizens, which is like the disinformation phenomenon.

The definition of propaganda may lack mentions of the way of diffusion, the novelty of the use of new technologies, etc., but the definition matches the existence of false or misleading content, the intention of the author to harm or to have economical interest from it, and it has definitely major impacts on the democracy and the rule of law, as preventing the individual to have access to truthful and objective information to build its opinion and make choices. Moreover, by not mentioning the means of diffusion, this definition is more timeless than the other terms.

CONCLUSION:

TABLE SUMMARIZING KEY ELEMENTS

	Advantage	**Disadvantage**
Information Warfare	Takes into account the characteristics of false information and the intention to cause harm or to mislead individuals.	Limited to military context
Fake News	Commonly known	Unprecise and too broad: may include opinions with which people disagree, poor quality journalism, etc.
Disinformation	False or misleading information to cause harm or for profit, taking into account new technologies aspects	Might be limited for future development
Misinformation	False or misleading information	No intention to cause harm or mislead individuals
Propaganda	False or misleading information to cause harm or for profits Intemporal	Old term with no reference to the specificity of the new technological means

[80] International Covenant on Civil and Political Rights, entry into force 23 March 1976:

Article 20: “1. Any propaganda for war shall be prohibited by law.

2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.”

After the wide spread of the term fake news, which has therefore been used to describe a lot of different things, from the spreading of false information to information or opinions with which public personalities disagree, scholars and experts needed a more precise terminology. The elements taken into account are i) the existence of a false information, which is either based on false facts, or misleading presentation of the facts; ii) the intention to cause harm or to make profit ; iii) the consequences on the individual's rights and dignity, and on the society security and integrity.

The term disinformation is used in the major part of recent publications analysing the phenomenon, as well as misinformation and propaganda. However, the term misinformation lacks the intentional element. In this regard, the author advises on the use either of the term disinformation or propaganda, and when the intentional element is not relevant, misinformation could also be used.

II. BALANCING INTERESTS: FREEDOM OF EXPRESSION AND NATIONAL SECURITY

The dissemination of intentional false information may have major consequences on the institution of a State by influencing its election process (e.g. US elections), or major political decisions (e.g. Brexit in the UK), or encouraging protest for destabilisation (Yellow vest jacket movement in France), or even for secession/annexation (e.g. Crimea in Ukraine and Cataluña). The issue is to find a way to protect State integrity by blocking foreign propaganda, while respecting freedom of expression and free movement of services. Article 11 in combination with Article 52(3) of the EU Charter has the same scope as Article 10 of the ECtHR[81]. By consequence, an analysis of the ECHR understanding of scope and meaning of freedom of expression in the context of disinformation is necessary (1). Then, in order to determine the need and opportunity of a EU action (3), the Member States (MS) current regulations must be scrutinized (2) to identify if a common approach exists and if their separate actions are sufficient.

1. The high protection of freedom of expression under the ECHR

1.1. The broad scope of freedom of expression

Different Articles of the ECHR are usually constructed in the same way: a first paragraph declaring the protection of the right and a second one presenting the limitation of this right. Article 10 of the ECHR is an exception, with a limitation already present in the third sentence of the first paragraph: “This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.” In the same paragraph, that promotes freedom of expression and the right to receive and impart information, the ECHR sets up the right for State to require license for broadcasting, which is a limitation of the freedom of speech in itself.

The ECtHR, in the case *Groppera Radio AG and others v. Switzerland*, first interpreted it as allowing States to limit broadcasting due to technical or legal difficulties. Indeed, the Convention was prepared at a time where there were a “limited number of available frequencies” and “major capital investment [was] required for building transmitters”. However, “since then, changed views and technical progress have resulted in the abolition of State monopolies”, and by

[81] ECJ, 4 May 2016, Philip Morris Brands and Others, C-547/14, paragraph 147

consequence, limitations based on technical or legal difficulties are harder to justify[82]. Even if the text of the ECHR provides the State with an opportunity to limit broadcasting, the ECtHR narrowed it, with time, to provide a broad protection of freedom of expression. The second aspect of this explicit reference to broadcasting in the first paragraph is that it allowed the ECtHR to include in the scope of freedom of expression not only the content but also the means of diffusion. As the right of broadcasting is “enshrined in the first two sentences of Article 10§1” there is “no need to make distinction according to the content of the programmes”[83].

The ECtHR has adopted a broad acceptation of the speech protected under Article 10, including all types of content (except illegal) without distinction of its author (natural or legal person[84]). However, the Court established distinctions according to the type of speech and some speeches are more protected than others. For example, political speeches are enjoying the highest protection with “little scope under Article 10§2 of the Convention for restrictions on political speech or on debate on matters of public interest”. On the contrary, regarding “commercial matters or advertising” the “States have a broad margin of appreciation”[85]. This distinction is relevant when the Court is conducting the classical control of proportionality, enshrined in paragraph 2 of Article 10.

Finally, Article 10 is applicable “regardless of frontiers”. In the *Ekin* case of 2001, the French authorities banned the “circulation, distribution and sale” of a Spanish book concerning Basque minority, constituting, in their view, a threat to public order because it was encouraging separatism and violence. The ECtHR held that “the exceptional circumstances in 1939 might have been justified tight control over foreign publications” but as the circumstances have changed, maintaining this system “would appear untenable”[86]. As the Court admits that war circumstances were justification to ban foreign publications, the Court may accept specific limitation where circumstances justify it, even if the wording of the Convention states “regardless of frontiers”. It is possible to relate the ban of foreign publications in time of war, with preoccupation against the dissemination of disinformation, as a potential justification to override the requirement “regardless of frontiers”. However, the Court maintains a strict control of the accepted limitations.

---

[82] ECHR, Groppera Radio AG and others v. Switzerland, judgment of 28 March 1990 (p. 60), confirmed by Autronic AG v. Switzerland, judgment of 22 May 1990

[83] Ibid Point 55

[84] ECHR, Autronic AG v. Switzerland, judgment of 22 May 1990, para. 47: “The Article (art. 10) applies to "everyone", whether natural or legal persons.”

[85] ECHR, Sekmadienis LTD v. Lithuania, 30 January 2018 (Point 73).

[86] ECHR, Ekin Association v France, 17 July 2001 (Point 62).

1.2. A strict control of the limitations

The ECtHR always considered Article 10 “as a whole” and that the limitation provided in the first paragraph “does not provide that licensing measures shall not otherwise be subject to the requirements of paragraph 2”[87]. The requirements of Article 10(2) constitute the classical control of proportionality where the ECtHR conducts a triple test: i) the interferences must be prescribed by law; ii) it must be necessary in a democratic society and; iii) the limitation has to be proportional to the objectives aimed by the measure.

1.2.1. Prescribed by law

The requirement “prescribed by law” reflects “that only the legislature, as a democratically elected body, should have the power to put in place measures that limit this fundamental right”[88]. Primary legislation, but also secondary legislation authorised by primary legislation meet the requirement. However, when assessing the first requirement, prescribed by law, the ECtHR does not limit itself to the existence of a law, but considers its “quality”[89], including its accessibility, foreseeability and its precision. For the States to be compliant with the ECtHR control, the restrictions provided by the law should be precise and clear enough regarding especially the objectives aimed. The precision and clarity must be present regarding the wording and definitions of the terms. However, when the balance between the other criteria - the legitimate aim and the necessity - reveals that the measure was not justified, the Court does not always elaborate on this first condition[90].

1.2.2. Necessary in a democratic society

The criteria “necessary in a democratic society” in the context of Article 10(2) can be generally justified by the need to ensure “national security, territorial integrity or public safety”. Disinformation affects the national security or territorial integrity as it can influence the citizens’ vote regarding major decisions (U.S elections, Brexit) but can also lead to secession (Crimea). The following analysis therefore will focus on the assessment of national security and territorial integrity.

---

[87] ECHR, Groppera Radio AG and others v. Switzerland, judgment of 28 March 1990

[88] “Freedom of Expression: A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights”, Toby Mendel, Executive Director Centre for Law and Democracy

[89] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 27 June 2017 (Point 142).

[90] ECHR, Autronic AG above mentioned, Point 57: “But it does not appear necessary to decide the question, since even supposing that the "prescribed by law" condition is satisfied, the Court comes to the conclusion that the interference was not justified (see paragraphs 60-63 below).”

Neither the Convention nor the ECtHR defines national security, even if present in different articles of the ECHR (Article 8, 10 and 11). The ECtHR even went further by recognising unnecessary having a "comprehensive definition of the principle of the interests of national security" because it "requires to be flexible" and subject to "interpretation and application" according to the practice[91]. In general, when it concerns national security, States enjoy a "wide margin of appreciation" and the Court limits its control[92]. However, the necessity control is not limited to the aim but must "corresponds to a pressing social need" which the Contracting parties may assess with a certain margin of appreciation, but the ECtHR is "empowered to give the final ruling"[93]. The ECtHR balances all these factors when conducting its final assessment: proportionality.

The EP Report of 2019 emphasizes that "the connection of an individual piece of fake news item to these goals [national security, territorial integrity, and public safety] may be very limited". Indeed, for example, an article about "total Russo phobia" in Lithuania[94], even if it may encourage hate and have, on the long run, impact on the state stability, it is difficult to link this one article to the objectives of maintaining internal peace and security. Therefore, the European Parliament advises to focus on the prohibition of concerted actions, which would "have a chance to withstand constitutional scrutiny"[95]. Indeed, the proof of an organised campaign with multiple articles from the same sources should be enough to prove the necessity of the restriction on freedom of expression.

1.2.3. The proportionality test

The proportionality control is the balance between, on one hand, the aim of the interference - here national security or territorial integrity, where States enjoy a wide margin of appreciation – and, on the other hand, the restriction of speech, which may enjoys different level of protection according to the nature of the speech and the means used to diffuse it. For a

[91] ECHR, Esbester v. the United Kingdom, 2 April 1993: http://hudoc.echr.coe.int/eng?i=001-1537

[92] See for example, ECHR, Leander v. Sweden, judgment of 26 March 1987, Series A No. 116, p59.

[93] ECHR, Öztürk v. Turkey [GC], No. 22479/93, judgment of 28 September 1999

[94] EUvsDisinfo, "Lithuania is afflicted by total russophobia", 13/05/2019: https://euvsdisinfo.eu/report/lithuania-is-struck-by-total-russophobia/ and original article: New Inform, "В Совфеде заявили, что Литву поразила «тотальная русофобия», 13 March 2019: https://newinform.com/173870-v-sovfede-zayavili-chto-litvu-porazila-totalnaya-rusofobiya

[95] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019 https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

measure to be proportionate, the State must demonstrate that none other less restrictive measure existed to achieve the objective.

Regarding the nature of the speech, the ECtHR affirmed the wide protection of "political speech or debate of questions of public interest" with "little scope under Article 10 para. 2 of the Convention for restrictions"[96]. Commercial speech enjoys also the protection of Article 10, nevertheless, it is subject to more restrictions, as the States enjoy a wider margin of appreciation[97]. Most of the content delivered in the context of disinformation is of political nature or a question of public interest and therefore benefits from the highest protection under Article 10 of the ECHR.

Another mixed category exists, which is the advertisement of political nature (or political speech of commercial nature). For this category, the ECtHR first approach consisted on considering mostly the political nature of the commercial and rejected bans on it as disproportionate[98]. However, the ECtHR seems to have taken another approach with the case *Animal Defender* of 2013. In this case, the Communications Act of 2003 of the UK provided a general prohibition on broadcasted (radio and television) political advertisement. The Court conducted less an assessment of the measure in itself, than of the general measures – the Communications Act of 2003. To determine its proportionality, the Court decided to assess "the legislative choices underlying" the general measure, including "the quality of the parliamentary and judicial review" and "the risk of abuse, if a general measure were to be relaxed". The Court, after a detailed examination on the condition of the adoption of the law, its limitations (restricted to certain medias, and to address specific risks), the absence of a European consensus regarding paid political advertising, and the necessity of a general measure to prevent the "risk of abuse and a risk of arbitrariness", declared the general measure not disproportionate[99].

However, the decision was only taken by a few majority, nine votes to eight, illustrating the diverging views and the difficulty to find a balance between the protection of political speech and the protection of the democratic society. In this case, the decision was motivated on "the danger of unequal access based on wealth and to political advertising as it was considered to go

---

[96] ECHR, Wingrove v. the United Kingdom, 25 November 1996, para. 58: "Whereas there is little scope under Article 10 para. 2 of the Convention (art. 10-2) for restrictions on political speech or on debate of questions of public interest"

[97] ECHR, Markt Intern Verlag Gmbh and Klaus Beermann v. Germany, 20 November 1989.

[98] ECHR, Verein Gegen Tierfabriken Schweiz (Vgt) v. Switzerland (No. 2), 30 June 2009.

[99] ECHR, Animal Defenders International V. The United Kingdom, 22 April 2013

to the heart of the democratic process"[100]. Indeed, allowing political advertisement presents the danger of leaving only the wealthiest and economic powerful groups to promote their ideas, which are necessarily biased in an advertisement. However, it is also possible to argue that most of political speeches are in any case biased and representing the views only of the person or political group behind it. And it is usually the wealthier that have the most important tribune to speak even outside advertisements, either directly through meetings, or broadcasted. The Joint dissident Opinion of the Judges Ziemele, Sajó, Kalaydjieva, Vučinić and De Gaetano goes in this way, arguing that "programming choices are not likely to stand on the side of NGOs which may represent minority or controversial views"[101]. The ECtHR decision for this case was also balanced by the limitation of the ban to some means of broadcasting, e.g. radio and television.

The second criterion to consider, when assessing the proportionality, is the source and means of diffusion of the speech. Concerning the source, the ECtHR has always emphasized the special role of the press, written or broadcasted, as "one of the best means of discovering and forming an opinion of the ideas and attitudes of political leaders"[102] and its role of "public watchdogs"[103]. NGOs are also benefitting from this qualification[104].

Regarding the type of broadcasting, the ECtHR has an ambiguous approach. On one hand, it emphasizes the special nature of radio and television "as familiar sources of entertainment in the intimacy of the home", and "recognizes the immediate and powerful effect of the broadcast media". Whereas even if Internet is a "powerful communication tools", nothing demonstrates that it is more influential than the broadcast media[105]. It seems that the Court considers that broadcasted information, as it is synchronized, has a greater impact than Internet, where the users may choose individually and at any time the content to watch[106].

On the other hand, the ECtHR ruled that Internet "will never be subject to the same regulations and control"[107] than radio and televisions. And the Court uses sometimes Internet to justify restrictions on other broadcasting media. Indeed, in the Case *Animal Defender*, the

---

[100] Ibid, par. 117

[101] Joint dissident Opinion of the Judges Ziemele, Sajó, Kalaydjieva, Vučinić and De Gaetano, par. 11-15.

[102] ECHR, Animal Defenders International v. The United Kingdom, 22 April 2013

[103] Lingens v Austria, 8 July 1986

[104] Case Animal Defenders above mentioned.

[105] Ibid

[106] Ibid

[107] ECHR, Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 5 May 2011

possibility for the NGO to publish its advertisement online or on printed media, made the ban on television not disproportionate.

The Court struggles to find a right balance between the growing importance of Internet, which in the majority of judges' opinion remains less powerful than radio and television. However, some of the Judges do not share this view. For example, Judges Spielmann and Laffranque wrote in their dissident opinion in the case *Animal Defenders*: "Information obtained through the use of the Internet and social networks is gradually having the same impact, if not more, as broadcasted information", and drawing conclusions that no special measures should be applied to the traditional broadcasting media[108].

However, the Courts position may change with the recent development and the influence of Internet in our daily life, taking into account also that for the younger users, Internet and Social Media are now the main sources of information. Indeed, according to the Eurobarometer, "Internet has overtaken radio in the media use of European citizens", 65% of the respondent are using Internet daily, and this proportion goes up to 93% and 87% respectively for the 15-24 and 25-39 age category[109].

2. The heterogeneous regulations of the Member States related to disinformation

In this section, three Member States will be compared: Lithuania, France and Germany, as those three States have adopted regulations in order to contain disinformation. German legislation have been largely mediatised, analysed and criticised as a breach to the fundamental rights to freedom of expression, which makes it interesting to study[110]. Lithuania has to face daily disinformation campaign from Russia and wrote down on its fundamental text – Constitution of the Republic of Lithuania – the prohibition of disinformation. Therefore, the law

---

[108] This struggle can also be found in the U.S Supreme Court case law. The Supreme Court in 1997 already recognised the importance of Internet, which "can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low cost capacity for communication of all kinds" Nevertheless, as the ECtHR, it considers it also less invasive than television and radio as the user chooses the content it is exposed to, so it has not this "invasive" characteristic as radio and television. In addition, Internet has never been subject to the same "regulation" and "government supervision" as the radio and television, which lead the Court to accept less limitation of the freedom of expression on Internet than in the other broadcasting media (see United States Supreme Court, Reno v. American Civil Liberties Union (96-511), Decided: June 26, 1997)

[109] Media use in the European Union, Standard Eurobarometer 88, Autumn 2017, Survey requested and co-ordinated by the European Commission,Directorate-General for Communication

[110] Foreign Policy, "Germany's Online Crackdowns Inspire the World's Dictators" Jacob Mchangama and Joelle Fiss, 6 November 2019: https://foreignpolicy.com/2019/11/06/germany-online-crackdowns-inspired-the-worlds-dictators-russia-venezuela-india/

and actions taken by Lithuania might be an inspiration for other States, which are starting to understand the reach of disinformation campaign. Finally, France adopted a specific law, limited to elections period, after the Presidential elections where the winning candidate – Emmanuel Macron – has been himself victim of targeted disinformation campaign, which, regarding the outcome of the elections, have been unsuccessful. Moreover, the other European Member States are, for now, still in the investigation phase or they put in place non-legislative measures such as task force (Denmark or UK), Internet platforms to alert citizens on the phenomenon (Italy, Belgium)[111]. The three selected States adopted legislation but with different definitions of the content aimed (2.2.1) and different measures (2.2.2) bringing different results in term of efficiency (2.2.3).

2.1. The absence of a common definition of disinformation in national legislations

The Lithuanian Constitution excludes explicitly disinformation, alongside criminal action, from the definition of freedom of expression: "Freedom to express convictions and to impart information shall be incompatible with criminal actions—incitement of national, racial, religious, or social hatred, violence and discrimination, with slander and disinformation" (Article 25). Lithuania was one of the first countries to take measures in order to suspend broadcasting for dissemination of false information[112]. The provisions are laid down in the "Law on the Provision of Information to the Public"[113]. In Article 2(13) disinformation is defined as: "intentionally disseminated false information" and Article 26 characterises it as a "serious professional misconduct". Article 19(2) prohibits the dissemination of disinformation. Only two criteria are necessary to qualify disinformation according to this law: the information has to be false, which corresponds to the first criteria identified in the first part and it has to be intentional. The law does not distinguish between the intentions behind the dissemination of false information, neither includes the consequences in the definition of disinformation.

French legislator adopted another approach in the "Law against the Manipulation of information" of December 2018[114]. The name of the law in itself designates manipulation of

---

[111] Poynter Website, "A Guide to anti-misinformation actions around the world": https://www.poynter.org/ifcn/anti-misinformation-actions/

[112] Lietuvos Respublikos Prezidentas, "Fight against Disinformation is EU priority", Press service, 2019-03-22: https://www.lrp.lt/en/press-centre/press-releases/fight-against-disinformation-is-eu-priority/32098

[113] "Law on the Provision of Information to the Public" or "Lietuvos Respublikos visuomenės informavimo įstatymas", 2 July 1996 – No I-1418, (As last amended on 26 April 2019 – No XIII-2088) https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr

[114] Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information: https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1201/jo/texte

information, but the content aimed is more precisely defined in the text of the law. The Law is limited to broadcasting services of a foreign State or under influence of a foreign State, which disseminates intentionally false information that may affect the sincerity of the elections of national scale (presidential, legislative, senatorial and European). In addition, after a judicial remedy conducted by the deputies, the French Constitutional Council made precision on the definition: a false information is inexact or misleading allegation or imputation of a fact (exclusion of opinions, parody, partial inaccuracy or simple exaggeration), which falsehood can be objectively demonstrated[115]. In addition to the condition of affecting the sincerity of the election, the Constitutional Council emphasized three conditions regarding the diffusion of false information: the diffusion must be artificial or automatized, massive and deliberate[116]. Moreover, the misleading or the inexact character of the information, or the risk on the sincerity of the vote, must be manifest. The French legislation, even if it does not name specifically disinformation, delimitates precisely the content aimed. It added additional conditions to fulfil than the one studied in the first part, and is limited to the specific aim of protecting the elections. The scope of the law is much more narrowed than the Lithuanian law.

Germany adopted the Network Enforcement Act (NetzDG, entry into force the 1st October 2017), which has been widely criticised as a clear breach of constitutional and European or international protection of the freedom of expression[117]. The provisions of the German NetzDG Act apply to "telemedia service providers" with "profit-making purposes", operating "internet platforms" understood as "social networks" with more than 2 million of registered users in Germany (Article 1). It concerns unlawful content by reference to the Criminal Code, which includes in addition to hate speech or defamation, some provisions related to disinformation. First, Section 86 of the Criminal code prohibits the "Dissemination of propaganda material of unconstitutional organisations" which is rather limited, as the author of the content must be an unconstitutional political party (Socialist Reich Party and Kommunistische Partei Deutschlands), or banned organization, and the material must be "written". This coincides with the definition of propaganda but not specifically disinformation, especially as it is limited to written content.

---

[115] Point 21 and 51, Décision n° 2018-773 DC du 20 décembre 2018, Loi relative à la lutte contre la manipulation de l'information, Available here : https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm

[116] Ibid

[117] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 1st June 2017 (Ref: OL DEU 1/2017): https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf

"Germany: Flawed Social Media Law, NetzDG is Wrong Response to Online Abuse", Human Rights Watch, 14 February 2018: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

"Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation", Victor Claussen

Secondly, the Section 100a prohibits "Treasonous forgery" for falsification or altered objects and reports, which is significant for "the external security of the Federal Republic of Germany or her relationships with a foreign power". This provision is limited to external aspects of security, and more related to diplomacy, which can be more related to information warfare than disinformation. Finally, Section 269 prohibits the "Forgery of data intended to provide proof" concerning "purposes of deception in legal commerce stores or modifies data". By prohibiting the dissemination of "propaganda" or of false objects and reports, which threaten the external security of Germany, the definition takes into account the consequences of the dissemination of false information. However, it narrows it so much to a very specific context that it misses the general aspects of disinformation: the dissemination of false information. Therefore, this law, on the contrary to Lithuanian and French law, is not targeting specifically disinformation.

2.2. The lack of common measures to tackle disinformation in national law

The Law on the Provision of Information lays down the functions of the Lithuanian Radio and Television Commission (LRTK), which can take different measures against the broadcasting services when they do not comply with the obligations of the law, especially Article 19 and prohibited speech. However, regarding disinformation prohibited under Article 19(2), it can only be sanctioned in combination with other violation, laid down in Article 19(1), especially, i) incitement to change the constitutional order of the Lithuanian Republic through the use of force, ii) attempts against the sovereignty, territorial integrity and political independence, and iii) war propaganda and hatred speech. Indeed, Article 31, which allows the LRTK to suspend broadcasting licence for 3 months, imposes a double condition: the information must have been prohibited under par. 1 and 2 of Article 19 and as a prerequisite, a fine must have been imposed on the broadcasting licence holder, according to Article 48(3). Yet, Article 48(3) only provides the possibility to impose a fine concerning the violation of the point 1, 2 and 3 of the first paragraph of Article 19, excluding the prohibition of disinformation, only present in the second paragraph. Indeed, in the Annual Report of 2017 of the LRTK, the summary of suspension of TV channels showed that it was based on "incitement to hatred and instigation of war" (Decision No. KS-41 and No. KS-83)[118]. Therefore, it is not disinformation that is sanctioned, but incitement to hatred and instigation of war, which can be based on the dissemination of false information, but, disinformation in itself is not tackled in this first provision.

[118] Radio and Television Commission of Lithuania, 2017 Annual Report https://www.rtk.lt/content/uploads/2018/05/ENG-LRTK-2017-m-ataskaita_o.pdf

A second provision related to Internet allows the Court to suspend or terminate the activities of a producer and/or disseminator of public information if it violates the provisions of Article 19(2), except for broadcaster and re-broadcaster of radio and television programme and audio-visual on-demand services (Article 52). Only the Court can decide on the suspension or termination of the activity of a producer or disseminator of disinformation, with the exclusion of major stakeholders (television and radio broadcaster). By consequence, the Lithuanian law tackles disinformation in a very limited perspective, even if the higher national text - the Constitution of Lithuania - prohibits it.

The French legislation provides different measures to counter the propagation of disinformation during election campaign. Firstly, it establishes a new legal procedure, open to public prosecutor, candidates, political party or group, or any person with an interest to act. They can ask the judge to take all necessary and proportionate measures to stop the dissemination of the false information. A judge has 48 hours to adjudicate, and if there is an appeal another 48 hours. (Article 1(2)[119]).

Secondly, it provides new powers to the French Regulator of Broadcasting (CSA) with possibility to refuse licensing for broadcasting the channel under the control or influence of a foreign state (use of concordant items of evidence: "faisceau d'indices") when the broadcasted programmes are jeopardising the fundamental interest of the Nation, including the regular functioning of its institution (Article 5). The law also lays down an exceptional procedure of unilateral termination for other broadcasting if their behaviours are altering the election outcomes by the diffusion of false information (Article 6 and 7).

Finally, the Law establishes new obligation for the platforms. They have to aggregate in a public record, accessible electronically for the public, the information related to paid accounts and advertisements (identification of the person, amount paid, etc.), as well as on the use of the

---

[119] Article 1(2) « Au début du chapitre VI du titre II, sont insérés des articles L. 163-1 et L. 163-2 ainsi rédigés : : « Art. L. 163-2.-I.-Pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises, lorsque des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne, le juge des référés peut, à la demande du ministère public, de tout candidat, de tout parti ou groupement politique ou de toute personne ayant intérêt à agir, et sans préjudice de la réparation du dommage subi, prescrire aux personnes physiques ou morales mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou, à défaut, à toute personne mentionnée au 1 du même I toutes mesures proportionnées et nécessaires pour faire cesser cette diffusion.

« II.-Le juge des référés se prononce dans un délai de quarante-huit heures à compter de la saisine.

« En cas d'appel, la cour se prononce dans un délai de quarante-huit heures à compter de la saisine.

« III.-Les actions fondées sur le présent article sont exclusivement portées devant un tribunal de grande instance et une cour d'appel déterminés par décret. »

personal data in regard of the promotion of such advertisement (Article 1). A new obligation of cooperation is also set up, which includes not exhaustively, an annual declaration and statement of the measures in place to fight against spreading false information (Article 11) and the possibility for the CSA to addressed to the platforms some recommendation with mandatory follow-up from the platforms providers (Article 12). They also have the obligation to make public statistics on the use of algorithm (Article 14) and to have a representative person based in France (Article 13).

The French legislation is limited in time by the context of elections. The new power of the CSA and the new judicial remedy are restricted to the 3 months preceding the vote. The main aspect of this law is to leave the French Administrative Regulator or the Court to rule and decide which content should be considered as disinformation. The platforms have a duty to cooperate and make some information accessible to the public. However, unlike the German law, which is presented below, the French regulation does not impose on them precise obligation to remove disinformation content. It only mentions some measures that can be put in place such as the fight against accounts disseminating massively false information (Article 11(I-3)).

The NetzDG Act puts the burden of taking down illegal content on the platform providers with an obligation to remove manifest unlawful content “within 24 hours” after receiving the complaint (Article 2(2)) and within 7 days for the non-manifest unlawful content. This removal must comply with an “effective and transparent procedure for handling complaints (Article 3(1)) and an obligation of immediate notification of the removal of illegal content and the reasons motivating it (Article 3(5)). The platforms providers also have to report on their efforts to counter illegal contents (Article 2). However, the possibility is left for the platforms providers to make an agreement with self-regulation institution, which will have the responsibility for analysing and removing illegal contents. Finally, in order to ensure compliance with this law, the non-respect of the mentioned provisions may be subject to a fine, up to 500.000 euros and, in some cases, up to 5 million euros. The law has an extra-territorial application as it applies even if the offence is not committed in Germany (Article 4).

The Law defines precisely in its first article the concerned online services providers, which have to provide internet platform to “enable users to share any content with other users or to make such content available to the public”, for profit-making purpose and with more than 2 million of registered users in Germany. It narrows the field of application and excludes different networks “such as business networks, professional and technical platforms, online game and

commercial website"[120]. Moreover, as mentioned above, the content related to disinformation is narrowed to very specific context. However, the approach taken by Germany raised many critics as it is similar to Russian approach used to censor speech online[121].

To sum up, the German NetzDG Act has been associated with the fight against disinformation, however the analysis conducted, demonstrates that it is mostly aiming other illegal content, except when disinformation is published by unconstitutional organisation or when it is significant to the external security of the State. The logic of this law is to put the burden on the private companies in order to remove illegal content. On the contrary, French and Lithuanian Law are specifically aiming disinformation (even with a different wording). However, in most cases, Lithuanian law, as the German law, cannot tackle disinformation by itself and must relates the spread of disinformation with other prohibited speech. Finally, French law, as the contrary to the two other laws, is aiming a specific context: the elections periods which narrowed its temporal application, but in this specific period the judges and the CSA have important power to take any proportionate measures to stop the dissemination of disinformation.

2.3. The assessment of the compatibility of the national approaches with the ECHR and their efficiency

2.3.1. Compatibility of national legal measures with the ECHR standards

Regarding the first criteria of the proportionality control of the ECHR – prescribed by law, the Lithuanian Law defines precisely the prohibited content (Article 19) as well as the concerned services. The competence of the LRTK is strictly limited by the law regarding time of suspension or amount of fines (up to 3% of last economic overall annual income or 100.000 euros if difficult to calculate Article 48(3)). All those elements suggest that the law will be complying with the first criteria: prescribed by law.

The French deputies were arguing in front of the Constitutional Council the lack of precision of the definition of the terms, which can be a sufficient reason for the ECtHR to rule the text incompatible with the Convention[122]. However, the French Constitutional Council ruled that the law, by being limited to the elections' periods, relates to the debate of general interest,

---

[120] "Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation" Victor Claussen

[121] "Government responses to malicious use of social media", Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard, November 2018, NATO STRATCOM COE

[122] ECHR, Hashman and Harrup v the United Kingdom, 25 November 1999, No. 25594/94

linked to the elections campaign, and by consequence is enough precise[123]. It is possible to argue that to some extent, during elections' periods, all debates are more or less of general interest, as it will necessarily affect candidates' positions and choice of electors. Nevertheless, with the interpretation of the French Constitutional Council, it is reasonable to think that the ECtHR will consider the term precise enough as delimited by the Constitutional Council.

The NetzDG Act should also comply with the first criteria, prescribed by law, as the term and relevant stakeholders are precisely defined.

Regarding the second criteria - necessary in a democratic society - Lithuanian law concerns the protection of National security, State integrity and maintaining internal order. Indeed, most of the decisions based on this law aimed at fighting pro-Russian content, which were inciting hatred or violence between communities, threatening internal order (Decision No. KS-41 and No. KS-83)[124].

Regarding the legitimate interest in the French law, the law aims at securing the electoral process and by consequences the democratic institutions, as illustrated by the preamble: "Establishing the existence of massive campaign of diffusion of false information, aiming at modifying the normal process of the elections by online communication service; and establishing the insufficiency of the current legislation to withdraw quickly the online content"[125]. As mentioned above, the protection of national integrity, which includes its institutions and the democratic process, is one of the legitimate interests admitted by the ECtHR.

The NetzDG Act is aiming content prohibited under the criminal code. It concerns various illegal speech (hate speech, defamation) or disinformation in combination with endangering the State security or internal order. As mentioned above, those interest are legitimate according to the ECtHR case law, with a wide margin of appreciation for the State.

---

[123] Point 21, Décision n° 2018-773 DC du 20 décembre 2018, Loi relative à la lutte contre la manipulation de l'information, Available here : https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm

[124] Radio and Television Commission of Lithuania, 2017 Annual Report https://www.rtk.lt/content/uploads/2018/05/ENG-LRTK-2017-m-ataskaita_o.pdf

[125] « Cette proposition de loi a été déposée à l'Assemblée nationale le 21 mars 2018 par Richard FERRAND et les députés membres du groupe La République en Marche et apparentés.

Constatant "l'existence de campagnes massives de diffusion de fausses informations destinées à modifier le cours normal du processus électoral par l'intermédiaire des services de communication en ligne" et considérant que les lois existantes sont "insuffisantes pour permettre le retrait rapide des contenus en ligne", les députés souhaitent par ce texte modifier le droit existant pour notamment permettre qu'une décision judiciaire puisse être rendue à bref délai pour faire cesser leur diffusion. »

Senat, Lutte contre la manipulation de l'information, Billet de l'Espace presse : http://www.senat.fr/dossier-legislatif/ppl17-623.html

Finally, regarding the proportionality, for imposing a fine in Lithuanian law, the decision must be based on the first paragraph of Article 19, limiting it to illegal content commonly accepted by the European States and excluding disinformation. For a suspension, a fine has to be imposed first, disinformation therefore must be combined with other illegal content. As a result, the measures and so the proportionality control are going to be based on incitement to hatred or violence, where there is a European consensus for illegality and where the national authorities have a wide margin of appreciation[126].

In France the deputies made multiple objections in front of the French Constitutional Council. Firstly, they consider the time period of 48 hours for a judge to take a decision to be unsuitable and risk to be instrumentalised[127]. Secondly, they argued that the derogation to freedom of expression was disproportionate regarding the particular importance of the political debate during elections campaign[128]. And finally, they raised doubts regarding the possibility to extend the law to some speeches, which are not aiming at causing harm or altering the sincerity of the vote such as parody or just mistakes[129]. However, the Constitutional Council rejected all those arguments: first, the aim of this law is to ensure the clarity of the debate and so to protect the importance of freedom of expression in these essential periods that are the elections[130]. It underlines the exclusion of parody, opinions, partial mistakes or exaggerations from the definition of the content aimed by the restrictions of the law[131]. Finally, the law prescribes to a judge to limit itself to take proportionate measures to stop the diffusion of false information, and so to take the least infringing measure[132]. Secondly, answering to the objections against the new powers of the CSA, the Constitutional Council ruled that the new measures established a balance between the necessity to protect national security and fundamental interests and freedom of expression and communication[133]. Therefore, with the French Constitutional Council interpretation and clarification, it is reasonable to think that the potential measures taken by the

---

[126] ECHR, Balsytė-Lideikienė v. Lithuania, 4 November 2008

[127] Point 11, Décision n° 2018-773 DC du 20 décembre 2018, Loi relative à la lutte contre la manipulation de l'information

[128] Ibid

[129] Ibid

[130] Point 18

[131] Point 21

[132] Point 25

[133] Point 35

judge or the CSA will comply with the ECtHR case law. This analysis is supported by the Organization for Security and Co-operation in Europe (OSCE)[134].

In Germany, the law puts the burden of analysing and removing illegal content on the private companies. The amount of the fine that can be imposed to the platform providers in case of non-removal is important. It may create an important "chilling effect"[135] on freedom of expression. This is reinforced considering that the list of the concerned criminal offenses is diverse with "violations that do not demand the same level of protection"[136], whereas, measures applied to all violations without any distinction. Finally, the time period for the platform to take down the content (24 hours or 7 days) is very short. Numerous commentators have raised concerns regarding the obligation to remove illegal content, which "promotes a de facto system of removal in case of doubt where content will be removed without scrutiny"[137]. Indeed, as the penalty is a fine of a huge amount, the social media are encouraged to remove content in case of doubts to avoid the penalty. David Kaye expressed his concerns as follow: "The short deadlines, coupled with the afore-mentioned severe penalties, could lead social networks to over-regulate expression - in particular, to delete legitimate expression, not susceptible to restriction under human rights law, as a precaution to avoid penalties. Such "pre-cautionary censorship"[138] would interfere with the right to seek, receive and impart information of all kinds on the Internet"[139]. As an illustration, few days after the adoption of the Law, some political figures have seen their publication removed such as the AFD vice-president[140]. Political speech being one of the most

---

[134] « Analyse juridique de la proposition de loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information », Commissioned by the office of the OSCE Representative on Freedom of the media from Laurence Franceschini, Independent Media Freedom Expert, November 2018: https://www.osce.org/fr/representative-on-freedom-of-media/408872?download=true

[135] Ibid and ECHR, Morice v. France (Application no. 29369/10), Strasbourg, 23 April 2015

[136] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 1st June 2017: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf

[137] "Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation" Victor Claussen

[138]See for example: An Analysis of Germany's NetzDG Law† Heidi Tworek, University of British Columbia Paddy Leerssen, Institute for Information Law, University of Amsterdam1 April 15, 2019, p4 https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

"Germany's Attempt to Fix Facebook Is Backfiring", Linda Kinstler, 18/05/2018, The Atlantic https://www.theatlantic.com/international/archive/2018/05/germany-facebook-afd/560435/

"The politics of deleting online hate speech", Ole Tangen Jr", 08/01/2018, DW Freedom: https://www.dw.com/en/the-politics-of-deleting-online-hate-speech/a-42030848

[139] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 1st June 2017: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf

[140] Tweet suppressed:"Was zur Hölle ist in diesem Land los? Wieso twittert eine offizielle Polizeiseite aus NRW auf Arabisch. Meinen Sie, die barbarischen, muslimischen, gruppenvergewaltigenden Männerhorden so zu besänftigen?"

protected speeches under the ECtHR case law, having it removed from social media might qualify the law and its measures as disproportionate especially since there is no judicial remedy to contest it.

To sum up, Lithuanian and French law should comply with the ECHR as providing a proportionate balance between the limitation of free speech for national security and integrity interest, and the respect of the fundamental right of expression. However, the German Law, by putting the burden on the private companies associated to the risk of an important fine and the absence of a judicial remedy, might conduct to a disproportionate restriction of free speech, especially regarding controversial political speech.

2.3.2. The efficiency of the national legislations to tackle disinformation

As it was mentioned, Lithuanian Constitution explicitly prohibits the dissemination of disinformation. However, as explained previously, the Law on the Provision of Information to the Public does not provide the LRTK the possibility to act against disinformation solely. It must be connected to other prohibited speech related to endangering national security, internal order or State integrity. For this reason, decision of the LRTK are mostly based on incitement to hatred or violence. However, disinformation can be damageable for the State even without incitement to hatred or violence, solely by introducing distrust and discontent among population with the dissemination of false information as demonstrated in the National Threat Assessment of 2019 of the State Security Department of Lithuania[141]. Therefore, the reach of the Lithuanian Law on Public Information appears rather limited regarding the measures for tackling dissemination of disinformation.

The French Law, as the Lithuanian law, puts the responsibility for tackling disinformation content on the Administrative Regulator or on the Court. However, as noted by some authors, it concerns only the election period: quid of the non-election periods?[142] Moreover, the French legislation had already specific disposition regarding the prohibition of publishing false content in the Law for the Freedom Press of 1881, Article 27. However, in practice, the law was almost never applied as the conditions for the judicial remedy were too narrowed. This is one of the arguments of the French government regarding the necessity of a new law, to implement an effective and swift judicial remedy to remove misleading content

[141] National Threat Assessment 2019, State Security Department of the Republic of Lithuania, Vilnius 2019 https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf

[142] "Fake news, infox, quelles réponses juridiques ? », Myriam Quéméner, Magistrat - Docteur en droit, Dalloz IP/IT 2019 p.178

presenting a risk for the election process. However, some concerns have been raised regarding this swift judicial remedy. First, it is commonly known that the French jurisdictions are already overloaded[143], and this new judicial remedy is opened to a wide variety of actors, which will put more burden on the French jurisdictions. Secondly, false information might be difficult to prove as emphasized by the report of the OSCE[144]. Indeed, during the 2017 presidential elections, the candidate Emmanuel Macron has been victim of a false information regarding a bank account in Caiman Islands: how the judge will be able to assess the truthfulness of such statement within 48 hours when it normally takes months of investigations? As the judicial remedy is limited to manifest false statement then, if a statement needs months of investigations, the judge cannot prevent its dissemination. However, this kind of statement, which falsity cannot be easily demonstrated, is harmful, especially in the election period. Finally, most of the authors agreed on the limitation of a French approach as internet has no frontiers and are advocating for a European approach[145].

Germany adopted a completely different approach by putting the burden of removing illegal content on the platform with huge fine in case of non-removal. The law is effective in the sense that with the risk of the fine the platforms providers will probably remove in extremis reported content. However, in regard of freedom of expression, the law presents important risks which might be disproportionate. Moreover, it does not aim at fighting disinformation in itself, but mostly disinformation in combination with other illegal speech. Therefore, the law might be efficient to remove illegal contents such as hate speech and defamation but not that much regarding disinformation.

Therefore, as Petra Bárd and Judit Bayer emphasize, the Member States are applying different solutions "resulting in divergent practices in an area that belongs under Community

---

[143] « Manque de moyens, surcharge... les déficits criants de la justice française », Jean-Baptiste Jacquin, 4 October 2018, Le Monde : https://www.lemonde.fr/police-justice/article/2018/10/04/manque-de-moyens-surcharge-les-deficits-criants-de-la-justice-francaise_5364483_1653578.html

[144] « Analyse juridique de la proposition de loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information », Commissioned by the Office of the OSCE Representative on Freedom of the Media from Laurence Franceschini, Independent Media Freedom Expert, November 2018 (p 15).

[145] Ibid, and also: « Fake news : une loi polémique, qui pose plus de questions qu'elle n'en résout », Diane de Bellescize, Professeur émérite de l'Université du Havre, Dalloz Constitutions 2018 p.559 and also : Rapport d'information déposé par la Commission des affaires européennes, portant observations sur les proposition de loi organique et proposition de loi relatives à la lutte contre les fausses informations (nos 772 et 799), présenté par M. Pieyre-Alexandre ANGLADE, Député

legislation"[146]. A EU approach in harmonising and ensuring the efficiency of the policy regarding tackling down disinformation would be appreciate, however, the main question is whether the EU has competence to do it and if so, to which extent (Chapter 3).

CONCLUSION:

The Member States have the possibility to restrict freedom of expression as any other rights of the ECHR and the EU Charter, but freedom of expression entails a specific dimension as the basis of the democratic society and a pre-requisite for the exercise of other rights. Limitations based on the principle of National security or State integrity, must be prescribed by law, necessary and proportionate. To ensure the compliance with those conditions, States must define precisely the understanding of disinformation. They must emphasize the existence of a pressing social need to protect national security or State integrity. Finally, the measures must remain proportionate, meaning, none other less restrictive measure would have achieved the same result. In this proportionality assessment, the States must consider the nature of the speech, which in case of disinformation will probably benefits from the highest protection as a speech of political nature or general interest. They must also take into account the specificities of the means of diffusion with less regulation admitted for Internet than for radio and television, which historically have been subject to more governmental regulations.

The comparative analysis between the French, German and Lithuanian legislation, leads to the conclusion that the appreciation and definition of disinformation defers between those three States. Germany does not consider and prohibit disinformation in itself, but its combination with other prohibited actions (diffusion of content by unconstitutional organization or representing a risk for the external security of the State). Lithuanian law defines it as intentional dissemination of false information, whereas, France narrows it by taking into account the way of diffusion which must be automated or artificial, massive and deliberate, and the effect, which must present a risk for the sincerity of the election. Regarding the measures, Germany has the most controversial approach, with the responsibility put on the private companies and the absence of judicial remedy in case of wrong removal of illegal content. Lithuanian and French law provide, their respective National Regulator Authority for Audio-visual content (LRTK and CSA), the possibility to remove such content or to cancel license. Both are limited but in different ways: the LRTK can only suspend broadcasting of disinformation in combination with

---

[146] Petra Bárd, Judit Bayer, A comparative analysis of media freedom and pluralism in the EU Member States, research paper for the Policy Department C: Citizens' Rights And Constitutional Affairs. OLDALSZÁM. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571376/IPOL_STU(2016)571376_EN.pdf

other infringements, whereas the French law is limited to elections' period. Finally, the Court have also some competences in both laws. For the Lithuanian Law, the Court is competent when it concerns Internet services, exception of the one related to broadcasting programs. For the French law, the judge has to act within 48 hours after the request, and can therefore act only against manifest false or misleading content, or presenting a manifest risk to affect the sincerity of the election.

Finally, these three legislations present all general limitations. First of all, the inherent territorial limitation for content that can be created and coming from other States. In this regard, the German law explicitly mentions its extra-territorial application, as it can also applies to acts committed outside of Germany. The question remains on how in practice it would be applied. Secondly, by having different approaches and meanings of disinformation, the internal digital market might be affected, with an asymmetric protection of the speech or national interest, which could justify a EU approach.

III. THE OPPORTUNITY OF A EUROPEAN UNION ACTION

The EU can only act within the strict limitation of its competence. Therefore, before discussing potential measures of the EU (2) it is necessary to conduct the analysis on the extent of its competence in this matter (1).

1. The European Union competences and existing regulations related to disinformation

1.1. Security and integrity: the external competence of the EU

The Treaty of the European Union (TEU), Article 4(2) mentions the "essential State functions" which include "the territorial integrity of the State, maintaining law and order and safeguarding national security". However, National security "remains the sole responsibility of each Member States": the EU is therefore incompetent regarding national security, which means that "EU law, including the Charter of Fundamental Rights of the EU will not apply"[147]. The EU and the European Court of Justice (ECJ) have not defined clearly, what National security is. The ECJ only stated that National security "constitutes activities of the State or of State authorities unrelated to the fields of activity of individuals"[148]. So, each State develops its own definition and understanding of national security, which can include the protection of its fundamental value (Austria), protection of the democratic institutions, life, health and property in a context of exceptional circumstances (Czech Republic and France), sovereignty and the democratic order (Germany), etc.[149]. The Council of Bars and Law Societies of Europe (CCBE) sums up all those distinctions in one definition including "the internal and external security of the State" consisting of the sovereignty of the State, the integrity of its territory, its institutions and its critical infrastructure, the protection of the democratic order of the State, the protection of its citizens

---

[147] CCBE Recommendations on the protection of fundamental rights in the context of 'national security', 2019, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

[148] ECJ, Productores de Música de España (Promusicae) v Telefónica de España SAU (C-275/06, judgment of 29 January 2008), par. 51.

[149] See the full analysis and survey done by the CCBE available here : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_Annex-to-CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

and residents against serious threats to their lives, health and human rights, the conduct and promotion of its foreign relations and commitment to the peaceful coexistence of nations”[150].

However, even if the EU is not competent for controlling National security in regard of the fundamental rights, it has its own competence regarding the External Action. The Council can act unanimously in the context of the Common Security and Defence Policy (Article 42(2) TEU). In this regard, the EU – or more exactly the Member States and the Council - has taken different actions such as the establishment of the Permanent Structured Cooperation (PESCO) in 2017 to increase cooperation in a variety of fields related to security, including cyber threats[151]. The European Commission has also adopted a Joint Framework on Countering Hybrid threats[152], and established the Rapid Alert System to counter disinformation[153] under the Common Security and Defence Policy (Article 42 TEU). Indeed, to improve the efficiency, States need to cooperate, and the EU, with those specific provisions regarding Common Security and Defence Policy, provides the structure for such cooperation.

Moreover, some threats to the security are coming from the suppression of frontiers – more precisely frontiers' controls – and so, in order to ensure the stability of the internal market, the EU may have a competence regarding not “national” but European security, which is incontestably linked to national security[154]. Indeed, Article 21 of the TEU states:

“*The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations, in order to:*

(a) safeguard its values, fundamental interests, security, independence and integrity;

(b) consolidate and support democracy, the rule of law, human rights and the principles of international law;”

---

[150] CCBE Recommendations on the protection of fundamental rights in the context of 'national security', 2019, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

[151] PESCO Website: https://pesco.europa.eu/

[152] Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

[153] EEAS, Factsheet: Rapid Alert System, 15/03/2019: https://eeas.europa.eu/headquarters/headQuarters-homepage/59644/factsheet-rapid-alert-system_en

[154] EEAS Website: “There is a strong link between what happens outside of the EU's borders and security within Europe. In a rapidly changing world, security challenges have become more complex, multidimensional and fluid. No EU Member State can face these threats alone. When it comes to security, the interests of all Member States are inseparably linked.” https://eeas.europa.eu/headquarters/headquarters-homepage/35285/eu-strengthens-cooperation-security-and-defence_en

The principle of subsidiarity may also be applied, as some incidents concerning security of one Member State can have a greater impact on "all sections of economic activity within the Single Market, the security and international relations of the Union"[155]. Even if the European Commission didn't find specific evidence revealing a specific disinformation campaign during EP elections of 2019, "the evidence collected revealed a continued and sustained disinformation activity by Russian sources aiming to suppress turnout and influence voter preferences"[156]. Yet, the action of the Member States separately might not be efficient enough to tackle the risk represented by those disinformation campaign, which would be the ground to justify a European action.

Finally, the complementarity principle can also apply. This principle applies when the European Commission identifies "a strong political will, an operational coordination and the development strategy for each recipient country"[157]. First, the Member States already expressed their will to strengthen security matter at European level[158] and secondly, the EU has a wide range of Agencies and mechanisms for crisis management already in place[159].

---

[155] Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises: ANNEX to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (Brussels, 13.9.2017)

[156] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Report on the implementation of the Action Plan Against Disinformation:, 14 June 2019
https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf

[157] Eur-lex, Complementarity between EC and Member State policies: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ar12005

[158] French President Macron, Discours de la Sorbonne: "En juin dernier, nous avons posé les bases de cette Europe de la Défense ; une coopération structurée permanente, permettant de prendre des engagements accrus, d'avancer ensemble et de mieux nous coordonner ; mais aussi un Fonds européen de défense afin de financer nos capacités et notre recherche. Ce socle indispensable, nous sommes en train de lui donner un contenu, à travers les échanges des différents Etats-membres qui souhaitent avancer en cette direction. »

Foreign Policy, "Europe is Ready for Its Own Army", Azeem Ibrahim, 5 September 2019: "So it should not be surprising that France has been the first to call for the formation of a European army. What is new, is that most other Western European countries agree, and most significantly that Germany agrees. Merkel agrees, former German Defense Minister and incoming President of the European Commission Ursula von der Leyen agrees" https://foreignpolicy.com/2019/09/05/europe-is-ready-for-its-own-army/

[159] Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises: ANNEX to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (Brussels, 13.9.2017):

Integrated Political Crisis Response (IPCR) arrangements, ARGUS, and the EEAS Crisis Response, NIS Directive, the CSIRTs Network,

Agencies and bodies namely the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre at Europol (Europol/EC3), the EU Intelligence Analysis Centre (INTCEN), EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (SITROOM) in INTCEN, working together as SIAC (the Single Intelligence Analysis Capacity); the EU Hybrid Fusion Cell (based in INTCEN); and the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU).

To conclude, the EU provides a structure for a regional cooperation, and starts taking actions regarding EU "national" security, even if it remains, for now, mostly a competence of the Member States.

1.2. The shared competence regarding the internal market of the European Union

Article 26(2) of the Treaty on the Functioning of the European Union (TFEU) establishes the principle of the free movement of services as one of the four components of the internal market. The Union has exclusive competence only to establish "the competition rules necessary for the functioning of the internal market" (Article 3(1) (b) TFEU) but shares the competence with the Member States regarding the other aspects of the internal market (Article 4(2) (a) TFEU). When the competences are shared, the Member States are in principle competent but only "to the extent that the Union has not exercised its competence". For the Union to exercise its competence, it has to respect the principle of subsidiarity (Article 5(3) TEU) according to which, the Union may act only when the action of the Member States is insufficient to achieve the objectives and will "be better achieved at the Union level" (Article 5(3) TEU). This principle must be applied in concordance with the principle of proportionality, according to which the "Union shall not exceed what is necessary to achieve the objectives of the treaties" (Article 5(4) TEU).

On this basis, the EU already introduced several directives and regulations. The two most relevant to this subject are, the Audio-visual media services (AVSM) Directive, adopted in 2010 and amended in 2018, which regulates broadcasting of AVMS (radio, television and concerned Internet services), and the E-commerce Directive of 2000, regulating the liability of hosting and related services. The EU based its intervention on the "existing and emerging disparities in Member States" which prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition" (Recital point 40 of the E-commerce Directive).

1.2.1. Consecration and limitation of the Country of Origin principle: the Audio-Visual Media Services Directive

In 2010, the EU adopted a first regulation to codify the provisions, regulations and practices, regarding the AVSM, in order to ensure the fair competition and the proper functioning

of the internal market[160]. The AVMS Directive have been amended in 2018, to include, in addition to the "classic" AVMS such as television, the "video-sharing platform service" which does not have an editorial responsibility, such as YouTube[161]. The amendment of 2018 aimed at taking into account the new technology development. However, it does not include the platform providers which content is not devoted to provide programmes or user-generated videos. Therefore, other social media, such as Facebook or Twitter, are excluded from the scope of this directive (Article 1). Indeed, the AVMS Directive designates "television-like services", similar to mass media and by consequence cannot apply to Social Media and other platform providers, which are more individual user's content[162], and provide a variety of services or type of content going beyond the audio-visual.

This Directive consecrates the Country of Origin (COO) principle with obligation for the Member States to "ensure freedom of reception" without restriction of the "retransmission on their territory of the audio-visual media services from other Member States" (Article 3). The second paragraph of Article 3 provides the possible limitation of this principle in case of "serious and grave risk of prejudice to public health" or if it "manifestly, seriously and gravely"[163] infringes provision of Article 6. Article 6 prohibits "incitement to violence or hatred", "public provocation to commit a terrorist offence" (Article 6) and "most harmful content such as gratuitous violence and pornography" (Article 6a). These limitations are the one accepted by the ECtHR and must answer the same proportionality test under EU law, because the EU Charter protects freedom of expression with the same scope than the ECHR (see above). The third paragraph of Article 3 provides the possibility of limitation, in addition to the previous mentioned infringement of Article 6, in case of a "serious and grave risk of prejudice to public security, including the safeguarding of national security and defence". The exceptions of this Article 3 par. 2 and 3 have to answer additional conditions, which are less strict regarding the third paragraph (national security). The first additional condition is the necessity to have at least one prior infringement during the previous 12 months (two prior infringements for the paragraph 2), and the Member States have to notify to "the media service provider, the Member States having jurisdiction and the Commission, the alleged infringement and the proportionate

---

[160] Preamble of the Directive 2010/13/EU of 10 March 2010, Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2010.095.01.0001.01.ENG&toc=OJ:L:2010:095:TOC

[161] Article 1 of the above mention directive and see case C-132/17 Peugeot Deutschland GmbH v Deutsche Umwelthilfe eV for the exclusion of Youtube from the scope of the Directive 2010/13

[162] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019

[163] Article 3(2)

measures intended to take". The Member States can take the measure and the Commission can only asked the Member States to put an end to those measures in case it finds it incompatible with EU law. On the contrary, for the first limitations, regarding public health, the State has to respect 1 month period and must fail in finding an amicable settlement before taking any measures. Paragraph 5 of Article 3 provides the possibility to take urgent measure after the first alleged infringement but must justify the emergency in its notification to the Commission.

In this regard, the accepted limitations to the COO principle in Article 3 are narrowed since in addition to the necessity to have a serious breach, some procedural conditions are required, even if those conditions are less strict regarding State security, in comparison with incitement to hatred or violence by itself. The COO principle does not accept limitation for the case of disinformation or propaganda, except if the State can demonstrate the serious and grave risk to national security.

In order to prevent the phenomenon of "forum shopping"[164], accordingly, third States might find ways to circumvent strict national legislation by using EU internal market and settling in another Member States with smoother legislation, Article 4(2) provides another possible limitation to the COO principle. Indeed, based on the principle of sincere cooperation, if the service of the AVMS is "wholly or mostly directed towards its territory" and the State of destination adopted "more detailed or stricter rules of general public interest", it can request the State of origin "to address any problems identified", by cooperating together to find a "mutually satisfactory solution". If the results appear to be unsatisfactory, and the AVMS chooses to establish itself in other States to avoid the jurisdiction of the concerned State (intentional element), the State of destination can adopt the appropriate measures against the media service provider (Article 4(3)). This reasoning could apply to the context of disinformation: a regulation prohibiting disinformation in the State of destination, would allow this State to limit the broadcasting of the AVMS, if it proves that the service is mostly directed towards its territory.

The ECJ had the opportunity, under the AVMS Directive, to interpret the criteria applicable in order to determine under which State's jurisdiction the service was established, as the material element (head office location) is not the only determining criteria. In the case of *Baltic Media Alliance Ltd v Lietuvos radijo ir televizijos komisija* of 2019[165], the channel NTV Mir Lithuania (NTV hereinafter) produced its content in Russia but distributes it through BMA,

[164] "Country of Origin Principle in the EU Market for Audiovisual Media Services: Consumer's Friend or Foe?" Herold, A. J Consum Policy (2008) 31: 5. https://doi.org/10.1007/s10603-007-9054-1

[165] ECJ, Baltic Media Alliance Ltd v Lietuvos Radijo ir Televizijos Komisija, Case C-622/17, 4 July 2019

a society based in the UK. Firstly, the Court recalled that the editorial responsibility, defined as "the exercise of effective control over the selection of the programmes and over their organisation" (point 40 and Article 1(1)(c) of the directive), was determining to qualify the AVMS (point 39). The existence of a license in a Member State is an indication but is not sufficient: the national court must assessed if "the person has the power to make a final decision as to the audio-visual offer as such, which presupposes that he has sufficient material and human resources available to him to be able to assume such responsibility" (point 43). The Court recalled Article 2(3)(c) of the directive accordingly: "if decisions on the audio-visual media service are taken in a third country, it shall be deemed to be established in the Member State concerned, provided that a significant part of the workforce involved in the pursuit of the audio-visual media service activity operates in that Member State". In this case the ECJ ruled that the BMA, established in UK was the media service provider (Point 58). The Lithuanian government invoked the application of Article 4 accordingly when the service was exclusively directed towards the territory of one Member State, the legislation of this State of destination should apply. However, as LRTK did not follow the special procedure provided for, the Court rejected, without discussing it, the possibility to apply the exception of Article 4.

So Member States retain the possibility to limit AVMS based on the COO principle, in order to protect their national legislation and interest. However, the limitations are restricted and subject to procedural conditions, in addition to the general protection of freedom of expression enshrine in the EU Charter, which leaves the member States with a small room for manoeuvre. In order to limit the dissemination of disinformation coming from a media service based in another Member State, the State of reception must demonstrate the serious risk against its national security. Yet, as mentioned above, it might be difficult for a State to demonstrate the serious harm of one piece of disinformation and should therefore, concentrate its efforts to tackle organised disinformation campaign.

1.2.2. The absence of responsibility of the hosting services: the E-commerce Directive

The E-commerce Directive of 2000[166] is particularly relevant in the context of disinformation. The EU, few years after the American and the Communication Decency Act (1996), Section 230, started regulating the Internet Service provider in 2000 with an immunity

[166] 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'), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

applying to the online service provider[167]. It includes the immunity regarding "hosting content" as long as the service provider did not have knowledge of the situation. When the service provider has the knowledge of the existence of illegal content, it must "act expeditiously" to remove the information (Article 14 (1) (b)). However, the directive prohibits the member states to "impose a general obligation on providers […] to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity" (Article 15 (1)). Members States can only "establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities" (Article 15 (2)). As an illustration, in the Case *Eva Glawischnig-Piesczek v Facebook Ireland*, the ECJ emphasizes that, the exemption of liability provided to the hosting provider under the E-commerce Directive, was not affecting the possibility for liability under direct injunctions adopted on the basis of the national law[168]. The exemption for the liability of the hosting providers are distinct from the obligation to comply with direct injunctions which can "consist of orders by courts or administrative authorities". Therefore, even if the hosting providers benefit from general exemption of liability regarding the information stored, and Member States are prohibited to take general obligations on providers (Article 15(1) of the E-commerce Directive), the hosting providers are still liable to comply with direct injunctions, or when they become aware of the existence of the illegal activity.

The Directive does not define illegal content or illegal activity, which by consequence, must be defined by the national law and will depend on each Member States. Nevertheless, the European Commission in 2016 indicated some content, which are considered to be illegal: hate speech and incitement to violence, terrorism and harmful content but it does not mention disinformation[169]. The Commission gave its position on the definition of online platforms and the challenge ahead, as part of its strategy regarding the Digital Single Market, but it is only an indication for the Member States and has no legal binding force (Article 288 TFEU).

Moreover, this directive does not address specifically the platform providers but by interpretation they have been assimilated to "hosting services". Indeed, in the beginning of the 21st Century, Internet was still at its first development and the EU had to "liberalise innovation

---

[167] 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')

[168] CJUE, Case C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Limited, 3 October 2019, and Recital 45 E-commerce Directive

[169] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM/2016/0288 final

and to create a safe and secure online environment"[170] for Internet Service Provider. However, at that time, the "Platform Provider"[171] such as the social media, but also all other platform services (Amazon, eBay, etc.) did not exist. The European Parliament express these issues as follow: "As soon as the directive was ready, it was outdated: it did not mention the new type of user interface that enabled anybody to publish content on the web". Therefore, the need of a revision makes no doubt as the e-commerce Directive is not taking into account the newest development of Internet Platforms and all the new services available online, and provides a too broad irresponsibility to the platforms which was not foreseeable at that time[172]. The economic power and general impact on public society of these new "intermediaries" questioned the rationale of such exemption[173]. Therefore, the need of at least an accurate legal framework considering the new legal category, by defining precisely the platform providers, their role and responsibility, makes no doubt. The US legislation corroborates it. Indeed, the Communication Decency Act, Section 230 of 1996 has been amended in 2018, by the "Stop Enabling Sex Traffickers Act" to include the obligation to remove content violating federal laws related to sex trafficking laws.

National Authorities[174] and European Parliament, as well as scholars and Social Network such as Facebook[175], are calling for a European or even international approach. Indeed, the online environment is not subject to the frontiers, and the national approach is not efficient enough, leaving place for the Union to act (subsidiarity principle). However, the current legal opinion is predominantly in favour of maintaining the regime of lack of responsibility of platform provider, even with the creation of a specific category for them, exception of the case when they became aware of the existence of the content, and should in this case remove it as soon as possible[176]. Indeed, the German example of a law imposing to the platform a strict time

---

[170] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019

[171] Ibid

[172] Ibid p81

[173] "Providers Liability: From the eCommerce Directive to the Future", Directorate General for Internal Policies, EP Report, 2017: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf

[174] « La réponse ne peut être qu'européenne » : Rapport d'information déposé par la Commission des affaires européennes, portant observations sur les proposition de loi organique et proposition de loi relatives à la lutte contre les fausses informations (nos 772 et 799), M. Pieyre-Alexandre ANGLADE, Député ;

[175] "I also believe a common global framework — rather than regulation that varies significantly by country and state — will ensure that the Internet does not get fractured, entrepreneurs can build products that serve everyone, and everyone gets the same protections": "The Internet needs new rules - Lets start in these four areas", Mark Zuckerberg, March 30, 2019: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

[176] Ibid

limit to remove content and with the risk of an important fine in case of non-removal, illustrated the dangerous “chilling effect” on freedom of expression as mentioned above.

2. The potential developments of a European Union action

2.1. The limits of the self-regulatory approach

2.1.1. The adoption of the Code of Good Practice on Disinformation: a first regulatory step

The European Commission with the cooperation of the main stakeholders (Facebook, Google, Twitter and trade associations such as the European Association of Communication Agencies) took the self-regulatory approach with the adoption of the Code of Good Practice in October 2018[177]. The actions were taken particularly in the view of the 2019 European Parliament elections. The code aimed specifically at “disinformation” defined as “verifiably false or misleading content which, cumulatively”, (a) "Is created, presented and disseminated for economic gain or to intentionally deceive the public"; and (b) "May cause public harm", intended as "threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security"[178]. The code excludes misleading advertising, errors, satire and parody. It excludes also “clearly identified partisan news and commentary”.

Regarding the commitment, the code as a self-regulatory approach leaves the signatories to decide themselves which provision they choose to commit. The individual signatory commitments are listed in the Annex 1. This choice of a code “a la carte” is justified by the existence of various stakeholders with different roles and products in relation with the fight against disinformation. However, a self-regulatory approach has already some limitations regarding its legal binding force and providing a framework with different engagements for every stakeholder might affect seriously its efficiency. Moreover, the Signatory can withdraw at any time, with as unique requirement to notify it to the Commission. And if one Signatory is not

---

And also Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers’ Deputies)

Or “Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation” Victor Claussen

[177] “EU Code of Practice on Disinformation”, European Commission, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[178] Preamble in reference to the European Commission Communication Tackling Online disinformation: a European approach” paragraph 2.1.

complying with its commitments, the only possible measure is to "invite such Signatory to withdraw from the Code"[179]. Therefore, the European Parliament[180] and some scholars[181] agree on the opportunity to provide a framework of self-regulation, leaving the platforms agreeing to participate and the extent of their participation. However, the self-regulatory approach might be insufficient as it depends only on the will of the Signatories. Moreover, the Sounding Board's, when delivering its opinion on 24th September 2018, believed that the delivered code "is by no means self-regulation" as it is missing "common approach, clear and meaningful commitments, measurable objectives" and there is no monitoring or enforcement tools[182]. The terminology used in this code is very careful regarding the reach of the commitment by making sure none is strictly binding. Finally, Aleksandra Kuczerawy points the absence of the possibility of judicial remedies when content has been wrongly removed[183].

For those reasons, and even before adopting this code, in its Communication of April 2018, the Commission expressed the possibility to take a regulatory approach in case of the unsatisfactory result from the self-regulation. Although during the first months of evaluation (January 2019 - May 2019) the Commission was highlighting the need to strengthen the effort that were mainly insufficient[184], in June 2019, after the European Parliament elections, the European Commission seemed satisfied: "all platforms have made progress with regard to the transparency of political advertising and public disclosure of such ads in libraries". The assessment of the effectiveness of the code is now due every year (in October).

---

[179] Title V. Signatories, of the Code of Practice on Disinformation

[180] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament Report, February 2019

[181] Dalloz Constitutions 2018 p.559, « Fake news : une loi polémique, qui pose plus de questions qu'elle n'en résout », Diane de Bellescize, Professeur émérite de l'Université du Havre or

« Analyse juridique de la proposition de loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information », Commissioned by the Office of the OSCE Representative on Freedom of the Media from Laurence Franceschini, Independent Media Freedom Expert, November 2018

[182] The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice, 24 September 2018

[183] "Reflections on the European self-regulatory code of conduct: will it be enough to curb online disinformation in upcoming campaigns?", Blog Administrator LSE, 14 February 2019: https://blogs.lse.ac.uk/medialse/2019/02/14/reflections-on-the-european-self-regulatory-code-of-conduct-will-it-be-enough-to-curb-online-disinformation-in-upcoming-campaigns/

[184] See monthly reports available on the Website of the Commission: January 2019, February 2019, March 2019, April 2019, May 2019, June 2019.

2.1.2. The assessment of the self-regulatory practices

The first annual report was published in October 2019[185]. It emphasizes the need for the Platform to deepen their efforts in regard of the empowerment of consumers and the cooperation with the research community, where "the provision of data and search tools to the research community is still episodic and arbitrary". However, the Code in general "has provided an opportunity for greater transparency into the platforms policies on disinformation as well as a framework for structured dialogue to monitor, improve and effectively implement those policies"[186].

The first commitment of this code concerns the scrutiny of ad placements[187] and more specifically policies to disrupt advertising and monetization incentives. Indeed, as a disinformation campaign usually represents a business or is at least profitable, the objective is to "reduce revenues of the purveyors of Disinformation"[188]. The first annual report recognises the effort of the platform but notes some negative points. First, the policies regarding advertising "are not necessarily related to the dissemination of disinformation" as they can concern only commercial matters. Secondly, the cooperation with other stakeholders, particularly fact-checker organisations and research community is not enough yet, to counter effectively disinformation. However, a new initiative to enhance cooperation between the stakeholders have started in June 2019, the Global Alliance for Responsible Media[189]. It is however too soon to analyse its impact.

The second commitment concerns "political advertising and issue-based advertising". Transparency regarding political advertising is essential, and the user should understand how it has been targeted[190]. Here, the platforms have to label clearly the content as such, the candidate or party paying for it and the amount paid. The political advertising should be clearly distinguishable from editorial content[191]. The platform should also make public the targeting criteria. However, here the report notes that for now, it is still incomplete. Moreover, only Facebook adopted a policy applicable at the EU level. Twitter makes distinction between the

[185] Code of Practice on Disinformation, First Annual Reports – October 2019: https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

[186] Ibid, p 1 Overview.

[187] II.A Code of Good Practice on Disinformation

[188] II.A Code of Good Practice on Disinformation in reference to the Communication of the Commission Tackling Online Disinformation point 3.1.1

[189] "Global Alliance for Responsible Media launches to address digital safety", 18 June 2019, World Federation of Advertisers: https://wfanet.org/knowledge/item/2019/06/18/Global-Alliance-for-Responsible-Media-launches-to-address-digital-safety

[190] II.B Code of Good Practice on Disinformation

[191] II.B.2 Code of Good Practice on Disinformation

country, which is problematic regarding the harmonisation and the effectiveness of the common market[192].

The third commitment concerns the "integrity of services"[193], which is related to closing fake accounts and ensuring the distinction between bots or AI accounts and human one. However, in regard of the fundamental rights for private life, and the importance of anonymity on Internet, the "Signatories should not be prohibited from enabling anonymous or pseudonymous use of accounts". The platforms have been actively acting against the fake accounts and bot-driven activity[194]. However, according to the report, some "further efforts are needed". Moreover, for now, the data are global and not specific to the EU, which make difficult the assessment of the efficiency of this policy.

The fourth commitment concerns "empowering consumers". Here, the code emphasizes the importance to find a balance between the fight against disinformation and the need to respect and protect the fundamental rights of expression, which prohibits deleting contents on the sole basis of its falsity. However, it is possible to "dilute the visibility" of such contents with "trustworthy content"[195] and it should be encouraged by the Signatories with tools for the users. The commitments here are more related to investment in new technologies to developed efficient tools and to cooperate with other relevant stakeholders, than precise actions. The annual report notes the insufficiency of the data provided in order to assess the impact of those new tools. Moreover, some tools are not available uniformly in all Member States, such as the NewsGuard Service of Microsoft only available in Italy, Germany, France and the UK, which is problematic regarding the harmonisation of the internal market[196].

Finally, the last commitment concerns the empowerment of the Research Community. Indeed, one problematic aspect is for the research community to access data while complying

---

[192] Code of Practice on Disinformation, First Annual Reports – October 2019, p7

[193] II.C. Code of Good Practice on Disinformation

[194] "Facebook, whose founder and chief executive, Mark Zuckerberg, recently gave evidence to a US Senate committee looking at disinformation, has said it disabled 2.2bn fake accounts in the first three months of 2019 and removed about 7,600 accounts, pages and groups engaged in "inauthentic behaviour". The Guardian, "EU disputes Facebook's claims of progress against fake accounts", Daniel Boffey, 29 October 2019: https://www.theguardian.com/world/2019/oct/29/europe-accuses-facebook-of-being-slow-to-remove-fake-accounts

And : "On integrity of services, Google reported taking down literally millions of YouTube channels for violating its misrepresentation and impersonation policies, while Facebook described in detail its efforts against "Coordinated Inauthentic Behavior" (including under a number of Russian-based campaigns) and noted that it took down 2.19 billion fake accounts (worldwide) during the first quarter of 2019, and Twitter reported challenging 76.6 million spam/bot/fake accounts and acting on another 2.3 million accounts reported by its users in the first five months of 2019 (again, worldwide)"

[195] II.D Code of Good Practice on Disinformation

[196] Code of Practice on Disinformation, First Annual Reports – October 2019, p10

with data privacy regulations. The platforms created tools, like specific library for the research community to access the data. However, the report notes the limited information of those data and the platform can always “alter or restrict access on a unilateral basis”. The possibility to make analysis of the data is of particular importance in order to have a better understanding of the phenomenon, the actors behind it and the impact of it. Therefore, the platforms should cooperate more with research community and make their data accessible more easily for them, in respect of the data protection laws[197].

Therefore, more efforts remain to be done by the platform providers. However, the code of good practice demonstrated the awareness of the platform providers and other relevant stakeholders on the necessity to tackle disinformation. Platforms providers are for now demonstrating mostly good will and faith in making efforts in this view. Nevertheless, the question remains on the perspective of such self-regulatory code. Indeed, there is no authority in charge of sanctioning the lack of measures, or failure to fulfil the commitments. The only possible sanction is to withdraw from the code, which the potential consequence is the “bad publicity” for the company. To pursue a self-regulatory approach, it would be important to have an authority, designated and agreed by the platform in order to make some recommendations and in some circumstances enforces the measures[198]. For now, the European Commission is asking the Signatories to provide regular reports on their efforts, in cooperation with the European Audio-Visual Observatory. However, the implementation of a specific authority to oversee and enforce the measures or potential recommendations might be relevant.

2.2. Towards a new system of responsibility for the platform providers

The new European Commission led by Ursela Von der Leyen, announced the adoption of a “new Digital Service Act”, regarding “liability and safety rules for digital platforms, services and products”[199], which should be a revision of the e-commerce Directive. She emphasizes the need to protect the EU from external interference, and to preserve the progress made by the

---

[197] Ibid, p 11-12

[198] Online Harms White Paper (April 2019) of UK proposes an independent regulator to oversee and enforced the compliance with the Duty of care.

Interim mission report “Regulation of social networks – Facebook experiment”, Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, proposing the creation of an Independent Administrative Authority to have a European check & Balance

[199] Political Guidelines for the Next European Commission 2019-2024: A Union that strives for more, My agenda for Europe, By candidate for President of the European Commission Ursula von der Leyen

digital services by tackling "issues such as disinformation and online hate message"[200]. She commits to prepare a European Democracy Action plan that will address the threats of external intervention, including "legislative proposals to ensure greater transparency on paid political advertising and clearer rules on the financing of European political parties"[201]. Therefore, the new Commission will probably take into consideration the commitments included in the Code of Good Practice against Disinformation to make them legally binding. Remains the question on the future definition of the platforms and the extent of their liability.

The revision of the e-commerce Directive regarding platforms providers does not induce the necessity of a broader responsibility regarding taking down illegal content published by a third party, but to set up clear and precise limitation of their roles and obligations.

The first element in this regard is the creation of a specific category for "Platform providers" as named by the European Parliament[202], which provides a "structure of communication but which are not responsible for how people use this structure". Indeed, for now, the e-commerce Directive is only considering the platform providers under the general category of hosting services, which is not tailored for them. The AVMS Directive specifically included "video-sharing platform provider" but it does not include the other platform providers. They have also been called "intermediaries" (Joint Declaration) or "online platforms" (Commission recommendation to tackle illegal content). But there is no harmonised definition and category, which leads to confusion. The revision should establish a new distinct category, should define it, and should apply it to the other existing regulations. The approach and definition should take into account the different nature of online platforms. Therefore, the proposal from the European Parliament to designate them as "platform providers" seems clear enough, and covers the different types of services provided by the platforms, different from the hosting services. It should include their function of offering a platform for individual to express or being in relation with other services, as well as the aspect of the collection of personal data and use of algorithm.

Secondly, the Internet Platform providers should only "be responsible for their own actions and not for their clients". The European Parliament advocates for adopting the notice-and-notice approach instead of the notice-and-taking-down approach. The first one, chosen by

---

[200] Ibid

[201] Ibid

[202] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, Report requested by LIBE Committee: http://www.europarl.europa.eu/supporting-analyses

Canada in the enactment of Bill C-11[203] (regarding copyrights), imposes to the platforms the only obligation to "transfer" the notice received by a user regarding some illegal or infringing content, to the author of such contents[204]. However, the obligation of the platforms stops here. On the contrary, the notice-and-take-down approach, adopted by the US and the European Commission in the Code of Good Practice against disinformation, puts on the platform the obligation to remove such prohibited content.

The first approach is "more respectful of freedom of expression"[205], however, in the author's opinion, is not efficient enough to create a safe online environment and tackle disinformation campaign. Indeed, a lot of uncertainty remains with the notice-and-notice procedure regarding the obligations of the platforms[206]. It usually depends on the platforms own private regulations and internal rules. Therefore, different levels of protection might be applied according to the platforms if the notice-and-notice procedure is adopted. Moreover, online content is already very difficult to eliminate as, once it has been published, multiple copies of this content may exist, and it becomes "viral" in the very first hours following its publication. Therefore, the time to notice the platform the existence of illegal content, time to transmit this notice, time to wait for measures from the author, before finally taking some measures by itself, it might be already too late to fix the damages, and not efficient enough to tackle disinformation.

Nevertheless, one safeguard against the notice-and-take-down regimes, that does not exist for now, would be the obligation for the platforms providers to organise a procedure of appeal against such removal of content, in case of mis-judgement, with the possibility to repost the content. It would be also possible to combine these two regimes. First, with an obligation of notice-and-taking-down, when the content is manifestly prohibited (illegal or harmful including disinformation), or when there is a manifest risk of harm or threat to public security[207]. Secondly,

---

[203] Statutes of Canada 2012, Chapter 20, An Act to amend the Copyright Act, assented to 29th June, 2012, BILL C-11 https://www.parl.ca/Content/Bills/411/Government/C-11/C-11_4/C-11_4.PDF

[204] Petra Bárd, Judit Bayer, A comparative analysis of media freedom and pluralism in the EU Member States, research paper for the Policy Department C: Citizens' Rights And Constitutional Affairs. OLDALSZÁM. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571376/IPOL_STU(2016)571376_EN.pdf

[205] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, Report requested by LIBE Committee: http://www.europarl.europa.eu/supporting-analyses

[206] Online Infringement: Canadian "Notice and Notice" vs US "Notice and Takedown", 27 June 2012: http://www.entertainmentmedialawsignal.com/online-infringement-canadian-notice-and-notice-vs-us-notice-and-takedown

[207] Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, Report requested by LIBE Committee, p147

when it is not manifest, to use the notice-and-notice approach, providing also time for the platform to investigate on the risks of such content[208].

Thirdly, as major information provider, the platforms should be liable regarding the transparency of their algorithms, advertisements and use of personal data[209]. In this regard, they could be subject to obligation of neutrality[210] and non-discrimination (Article 21 EU Charter), meaning to set up objective algorithm not discriminative according to the place of residence, religion, race, etc., enforceable by National, European, or Independent authorities. The advertisement should be subject to clear rule with, for example, the possibility to impose label to distinguish between political advertising, private advertising, political or “influencer” speech[211], etc. as mentioned in the Code of Good practice, but not enforceable. Finally, regarding the creation of fake accounts, the balance is difficult to operate between limiting them to real person while the “user should be allowed to use platform service anonymously”[212].

To sum up, the necessity of a revision of the current existing directives is making no doubt, regarding at least the definition of the platform providers. It would be appreciable to have also a harmonisation of the minimum responsibility of those platforms, especially regarding the transparency of the algorithm, the paid advertising. Regarding disinformation specifically, the cooperation with the research community with especially the provision of data is essential in order to have a better understanding of the phenomenon. Finally, concerning the responsibility, it would be in the interest of effectiveness and efficiency to have a harmonisation at the European level of the regime, between the notice-and-notice or notice-and-take-down regimes, and to have the same level of protection of rights.

---

[208] Ibid, p 145 and 147

[209] Ibid

[210] Regulation (EU) 2015/2120 of the European Parliament and of the Council, of 25 November 2015, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, Point 2 of the preamble.

[211] EP Report 2019 above mention point 160, p 88

[212] Ibid, p. 89

CONCLUSION:

1. The dissemination of false information is characterised firstly by the falsity or the misleading character of the information, the intention to cause harm or make profit and the consequences on the individual fundamental rights or society integrity. The term disinformation is used in the major publications but remains under-used by the national legislations. Among the three analysed States, only Lithuania is using the term disinformation, however it is not taking into account the consequences of the spread of it in the definition provided in the Law on the Provision of Information to the Public. The French legislation is using the term false information and associate specific characteristics to it, to narrow its scope of application, assimilating it to disinformation in the context of elections, but without using a specific terminology. Finally, Germany is mostly aiming propaganda and falsification of official documents, but not the newest development of disinformation as endangering for example the democratic process.

2. Freedom of expression, which includes the right to receive and impart information, enjoys an important protection from the ECtHR and by assimilation, by the EU Charter, especially political speech diffused on Internet as a domain where the ECtHR accepts only few restrictions, on the contrary to radio and television. However, States keep a wide margin of appreciation when limiting freedom of expression in order to protect state security and integrity. In order to block foreign content disseminating disinformation, and to comply with the ECtHR standard of protection of freedom of expression, the State must base its measure on a law, demonstrate its necessity regarding especially a "pressing social need" and keep it proportionate. In this regard, the German NetzDG Act raises concerns regarding the disproportionality of the limitations on freedom of expression, by putting the responsibility of removing illegal content on the private companies, in a strict time-limit with important fine in case of non-compliance

3. The comparative analysis of French, German and Lithuanian law demonstrates that there is no systematic approach to counter disinformation. The definition and understanding of the term disinformation differ, as well as the measures in place. The Lithuanian legislation even if it prohibits clearly disinformation, does not allow the LRTK to take efficient measure on the sole basis of disinformation: it has to be combined with other prohibited speech, such as hate speech or incitement to violence. Finally, the French law is limited in time to elections' periods, and narrowed by the necessity to prove the character manifest either of the risk of the false information, or of the false information itself.

4. The EU already make use of the shared competences regarding the internal market, by adopting the AVSM Directive and the e-commerce Directive. The first one aims at ensuring the respect of the internal market, by imposing the respect of the COO principle. However, some

exceptions remain possible for the Member States to limit the application of this principle, allowing them to block foreign content coming from another European States in the name of national interests. The main limitation which could be applicable to the case of disinformation concerns AVSM directed wholly or mostly towards one Member State which do not have in principle jurisdiction. In this case, the destination State could block disinformation content if it has a law to base its decision on. The harmonisation and therefore the achievement of the Internal market would be more complete by the acceptation at the European level of disinformation as a prohibited content, which would avoid different level of legislation and protection of speech.

5. The e-commerce Directive which provides an immunity to hosting services has to be revised, in particular regarding the definition and the regime applicable to the platform providers. It does not imply necessarily to impose the responsibility on the platform providers of the removal of prohibited content, as it might represent a disproportionate burden on them (e.g. German NetzDG Act), but at least some obligations of transparency and neutrality regarding the algorithm and paid advertising.

6. Finally, the adoption of a Code of Good Practice on Disinformation is an appreciable first initiative, but need to be deepened. Either by the acceptation of the stakeholders to voluntary submit to an independent authority to oversee, make recommendation and in fine, enforce this code, or by the adoption, by the EU, of an enforceable regulation. The efforts should be particularly focused on the transparency of the algorithms of the platforms and of the paid advertising content.

Legal Text

1. Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises: Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (Brussels, 13.9.2017): https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF

2. Communication Decency Act, 47 U.S. Code § 230: https://www.govinfo.gov/content/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec230.pdf

3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling online disinformation: a European Approach*, Brussels, 26/04/2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

4. Communication from the Commission of 6 May 1999 on complementarity between Community and Member State policies on development cooperation - COM(99)218 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ar12005

5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, COM/2016/0288 final

6. Déclaration des Droits de l'Homme et du Citoyen, 1789: https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789

7. Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5

8. 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'): https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

9. Directive 2010/13/EU of 10 March 2010, Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2010.095.01.0001.01.ENG&toc=OJ:L:2010:095:TOC

10. Directive (EU) 2018/1808 of the European Parliament and of the Council, of 14 November 2018, amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of

audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities:
https://eur-lex.europa.eu/eli/dir/2018/1808/oj

11. EU Charter of Fundamental Rights, 2000:

https://www.europarl.europa.eu/charter/pdf/text_en.pdf

12. "EU Code of Practice on Disinformation", European Commission:
https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

13. European Convention on Human Rights, 1950:

https://www.echr.coe.int/Documents/Convention_ENG.pdf

14. European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP)):
https://www.europarl.europa.eu/doceo/document/B-8-2018-0480_EN.html

15. European Parliament resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)):
https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.html

16. German Criminal Code: Strafgesetzbuch (StGB)

17. International Code of Journalistic Ethics of 1983:
https://accountablejournalism.org/ethics-codes/International-Principles

18. International Covenant on Civil and Political Rights, 1966:
https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

19. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation, Brussels, 5/12/2018:
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018JC0036

20. Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. https://www.osce.org/fom/302796?download=true

21. Law n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information,

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id

22. Law proposal adopted by the National Parliament to fight against hateful content online, n° 645, of 9 July 2019
http://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet

23. Law of 29 July 1881 on Freedom of Press (France) :
https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=E817546FE877FAADEC2B0EC08CD0F6A0.tplgfr36s_2?cidTexte=JORFTEXT000000877119&dateTexte=20170129

24. Lithuanian Constitution, 1992: https://www.lrs.lt/home/Konstitucija/Constitution.htm

25. Munich Declaration of the Rights and Duties of Journalists of 1971:
http://www.mediawise.org.uk/european-union/

26. Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), 1st September 2017, Entry into force the 1st October 2017

27. Republic of Lithuania, Law on the Provision of Information to the Public, 2 July 1996 – No I-1418, (As last amended on 26 April 2019 – No XIII-2088)

28. Regulation (EU) 2015/2120 of the European Parliament and of the Council, of 25 November 2015, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, Point 2 of the preamble:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120

29. Resolution 1003 (1993), Ethics of journalism, Parliamentary Assembly, Council of Europe.
https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16414&lang=en

30. Statutes of Canada 2012, Chapter 20, An Act to amend the Copyright Act, assented to 29th June, 2012, BILL C-11 https://www.parl.ca/Content/Bills/411/Government/C-11/C-11_4/C-11_4.PDF

31. The Council of the European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, 12 May 2015:
https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf

32. The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Commission on Human Rights, 28 September 1984:
https://www.refworld.org/docid/4672bc122.html

33. Universal Declaration of Human rights, 1948:

https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf

Case Law

34. ECHR, Handyside v. the United Kingdom, judgment of 7 December 1976, §49.
35. ECHR, Lingens v Austria, (Application no. 9815/82), 8 July 1986
36. ECHR, Leander v. Sweden, judgment of 26 March 1987, Series A No. 116, p59.
37. ECHR, Markt Intern Verlag Gmbh and Klaus Beermann v. Germany, (Application no. 10572/83), 20 November 1989
38. ECHR, Groppera Radio AG and others v. Switzerland, judgment of 28 March 1990
39. ECHR Autronic AG v. Switzerland, judgment of 22 May 1990, §61
40. ECHR, Thorgeir Thorgeirson v. Iceland, judgment of 25 June 1992
41. ECHR, Herczegfalvy v. Austria, judgment of 24 September 1992 §93 and 94
42. ECHR, Esbester v. the United Kingdom, 2 April 1993
43. ECHR, Prager and Oberschlick v. Austria judgment of 26 April 1995
44. ECHR, Wingrove v. the United Kingdom, (Application no. 17419/90), 25 November 1996
45. U.S. Supreme Court, Reno v. American Civil Liberties Union, Decided: June 26, 1997
46. ECHR, Öztürk v. Turkey [GC], No. 22479/93, judgment of 28 September 1999
47. ECHR, Hashman and Harrup v the United Kingdom, (No. 25594/94), 25 November 1999
48. ECHR, Lopes Gomes da Silva v. Portugal, judgment of 28 September 2000
49. ECHR, Ekin Association v France, 17 July 2001
50. ECHR, Erbakan v. Turkey judgment of 6 July 2006, § 56
51. ECJ, Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06, 29 January 2008
52. ECHR Balsytė-Lideikienė v. Lithuania, (Application no. 72596/01), 4 November 2008
53. ECHR, Verein Gegen Tierfabriken Schweiz (Vgt) v. Switzerland (No. 2), (Application no. 32772/02), 30 June 2009
54. ECHR, Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 5 May 2011
55. ECHR, Case of Animal Defenders International V. The United Kingdom, Application no. 48876/08, 22 April 2013
56. ECHR, Case of Morice v. France (Application no. 29369/10), 23 April 2015
57. ECJ, , Philip Morris Brands and Others, 4 May 2016, C 547/14
58. ECHR, Case of Ziembiński v. Poland (No. 2), (Application no. 1799/07), 5 July 2016
59. ECHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 27 June 2017
60. ECHR, Sekmadienis LTD v. Lithuania, (Application no. 69317/14), 30 January 2018

61. ECJ, Peugeot Deutschland GmbH v Deutsche Umwelthilfe eV, C-132/17, 21 February 2018

62. Décision n° 2018-773 DC du 20 décembre 2018, Loi relative à la lutte contre la manipulation de l'information, https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm

63. CJUE, Eva Glawischnig-Piesczek v Facebook Ireland Limited, Case C-18/18, 3 October 2019

Papers or Articles

64. "On Regulating International Propaganda: A Plea for Moderate Aims", Richard A. Falk, Source: Law and Contemporary Problems, Vol. 31, No. 3, International Control of Propaganda (Summer, 1966), pp. 622-634, Published by: Duke University School of Law, Stable URL: https://www.jstor.org/stable/1190743, Accessed: 08-11-2019 17:25 UTC

65. "International Propaganda and Minimum World Public Order", William V. O'Brien, Law and Contemporary Problems, Vol. 31, No. 3, International Control of Propaganda (Summer, 1966), pp. 589-600. Stable URL: https://www.jstor.org/stable/1190741

66. "The Present Status of Propaganda in International Law", Arthur Larson, Law and Contemporary Problems, Vol. 31, No. 3, International Control of Propaganda (Summer, 1966), pp. 439-451, Published by: Duke University School of Law, Stable URL: https://www.jstor.org/stable/1190732

67. "The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU, Towards an EU Copenhagen Mechanism", Carrera, S, Guild, E & Hernanz, N 2013Study, CEPS, Brussels

68. How to Stop Disinformation Lessons from Ukraine for the Wider World, by Marina Pesenti and Peter Pomerantsev, Transitions Forum, Beyond Propaganda | August 2016

69. Fake news and manipulated data, the new GDPR, and the future of information, Manny Cohen, Armadillo Business Information, 11/06/2017, UK, DOI: 10.1177/0266382117711328

70. Sarah Eskens, Natali Helberger & Judith Moeller (2017) *Challenged by news personalisation: five perspectives on the right to receive information*, Journal of Media Law, 9:2, 259-284, DOI: 10.1080/17577632.2017.1387353

71. "How to Counter Fake News? A taxonomy of anti-fake news approaches", by Alberto Alemanno, 20/04/2018

72. « Fake news : une loi polémique, qui pose plus de questions qu'elle n'en résout », Diane de Bellescize, Professeur émérite de l'Université du Havre, Dalloz Constitutions 2018 p.559

73. "Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation", Victor Claussen, 10/2018

74. La lutte contre les fausses informations sur internet: un jeu de lois, Boris Barraud, Revue Lamy Droit de l'Immatériel, n°154, 1er Decembre 2018.

75. Le Lamy droit des médias et de la communication, 218-4 - Nouvelles technologies et qualité de l'information

76. « Fake news, infox, quelles réponses juridiques ? » Myriam Quéméner, Magistrat - Docteur en droit, Dalloz IP/IT 2019 p.178

77. An Analysis of Germany's NetzDG Law† Heidi Tworek, University of British Columbia Paddy Leerssen, Institute for Information Law, University of Amsterdam1 April 15, 2019, p4 https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

78. Petra Bárd, Judit Bayer, A comparative analysis of media freedom and pluralism in the EU Member States, research paper for the Policy Department C: Citizens' Rights And Constitutional Affairs. OLDALSZÁM.
http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571376/IPOL_STU(2016)571376_EN.pdf

79. "Country of Origin Principle in the EU Market for Audiovisual Media Services: Consumer's Friend or Foe?" Herold, A. J Consum Policy (2008) 31: 5. https://doi.org/10.1007/s10603-007-9054-1

80. "Reflections on the European self-regulatory code of conduct: will it be enough to curb online disinformation in upcoming campaigns?", Blog Administrator LSE, 14 February 2019:
https://blogs.lse.ac.uk/medialse/2019/02/14/reflections-on-the-european-self-regulatory-code-of-conduct-will-it-be-enough-to-curb-online-disinformation-in-upcoming-campaigns/

81. "Bringing Propaganda Back into News Media Studies", Florian Zollmann Newcastle University, UK, Critical Sociology 2019, Vol. 45(3) 329 –345,
DOI: 10.1177/0896920517731134 journals.sagepub.com/home/crs

Reports

82. Standard Eurobarometer 88, Autumn 2017, Media use in the European Union, Survey requested and co-ordinated by the European Commission, Directorate-General for Communication.

83. "Providers Liability: From the eCommerce Directive to the Future", Directorate General for Internal Policies, EP Report, 2017
https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf

84. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Reference: OL DEU 1/2017, 1 June 2017, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf

85. "Tackling Misinformation in an Open Society: How to respond to misinformation and disinformation when the cure risks being worse than the disease", Full-Fact Paper (UK) – 2018

86. "A multi-dimensional approach to disinformation", Report of the independent High level Group on fake news and online disinformation, March 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

87. Rapport d'information déposé par la Commission des affaires européennes, portant observations sur : « Les proposition de loi organique et proposition de loi relatives à la lutte contre les fausses informations » (772 et 799), présenté par M. Pieyre-Alexandre ANGLADE, 16/05/2018 : http://www.assemblee-nationale.fr/15/europe/rap-info/i0949.asp

88. The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice, 24 September 2018: https://www.ebu.ch/files/live/sites/ebu/files/News/2018/09/Opinion%20of%20the%20Sounding%20Board.pdf

89. "Disinformation and 'fake news': Interim Report Contents, "Russian influence in political campaigns", 29/07/2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm#_idTextAnchor033

90. « Analyse juridique de la proposition de loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information », Commissioned by the Office of the OSCE Representative on Freedom of the Media from Laurence Franceschini, Independent Media Freedom Expert, November 2018

91. Journalism, fake news & disinformation: handbook for journalism education and training, UNESCO, Ireton, Cherilyn, Posetti, Julie, 2018, ISBN:978-92-3-100281-6 https://unesdoc.unesco.org/ark:/48223/pf0000265552

92. The Tallinn Guidelines on National Minorities and the Media in the Digital Age & Explanatory Note February 2019 OSCE HCNM

93. "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States", European Parliament Report, February 2019, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

94. Free Speech and the Regulation of Social Media Content, Congressional Research Service, March 27, 2019, https://fas.org/sgp/crs/misc/R45650.pdf

95. Avis du Comité économique et social européen relatif à la communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions Plan d'action contre la désinformation [JOIN(2018) 36 final], JOUE (C) 5 Juillet 2019,

96. National Threat Assessment 2019, State Security Department of the Republic of Lithuania, Vilnius 2019 https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf

97. Report of the 116-xx select Committee on Intelligence U.S. Senate on Russian active measures campaigns and interference in the 2016 US. Election. Volume 2: Russia's use of social media with additional views, 13/09/2019: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

98. CCBE Recommendations on the protection of fundamental rights in the context of 'national security', 2019, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

99. Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019: https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

100. "Freedom of Expression: A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights", Toby Mendel, Executive Director Centre for Law and Democracy

101. Radio and Television Commission of Lithuania, 2017 Annual Report https://www.rtk.lt/content/uploads/2018/05/ENG-LRTK-2017-m-ataskaita_o.pdf

102. "Government responses to malicious use of social media", Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard, November 2018, NATO STRATCOM COE

103. Online Harms White Paper (April 2019) of the United Kingdom

104. Interim mission report "Regulation of social networks – Facebook experiment", *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision*

http://www.iicom.org/images/iic/themes/news/Reports/French-social-media-framework---May-2019.pdf

105. Workshop on Digital Platforms and Fundamental Rights 12 June 2017, 13:30–17:30, BU-25 00/S1 Report

Journal Articles

106. "Clickbait: The changing face of online journalism" BBC, 2015, https://www.bbc.com/news/uk-wales-34213693

107. World Finance – The Voice of the Market, "Crimea doesn't pay: assessing the economic impact of Russia's annexation", Barclay Ballard, October 28 2019: https://www.worldfinance.com/strategy/crimea-doesnt-pay-assessing-the-economic-impact-of-russias-annexation

108. Adperfect, "How fake news is creating profits", October 26, 2017: https://www.adperfect.com/how-fake-news-is-creating-profits/

109. Reuters. David Ingram, "Facebook says 126 million Americans may have seen Russia-linked political posts", October 31 2017, https://www.reuters.com/article/us-usa-trump-russia-socialmedia/facebook-says-126-million-americans-may-have-seen-russia-linked-political-posts-idUSKBN1CZ2OI

110. "The politics of deleting online hate speech", Ole Tangen Jr", 08/01/2018, DW Freedom: https://www.dw.com/en/the-politics-of-deleting-online-hate-speech/a-42030848

111. "Germany: Flawed Social Media Law, NetzDG is Wrong Response to Online Abuse", 14/02/2018, Human Rights Watch: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

112. "Germany's Attempt to Fix Facebook Is Backfiring", Linda Kinstler, 18/05/2018, The Atlantic: https://www.theatlantic.com/international/archive/2018/05/germany-facebook-afd/560435/

113. "The Internet needs new rules - Lets start in these four areas", Mark Zuckerberg, March 30, 2019: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

114. Euractiv, « Les Gilets jaunes noyés sous les infox sur Facebook », Marion Candau, 13/03/2019 : https://www.euractiv.fr/section/elections/news/les-gilets-jaunes-noyes-dans-les-infox-sur-facebook/

115. The Guardian, “Facebook faces fresh questions over when it knew of data harvesting”, Carole Cadwalladr, 17/03/2019, https://www.theguardian.com/technology/2019/mar/16/facebook-fresh-questions-data-harvesting-cambridge-analytica

116. The Guardian, "EU disputes Facebook’s claims of progress against fake accounts”, Daniel Boffey, 29 October 2019: https://www.theguardian.com/world/2019/oct/29/europe-accuses-facebook-of-being-slow-to-remove-fake-accounts

117. The Economist, “Disinformation, Lithuanians are using software to fight back against fake news”, Martina Paukova, 24th October 2019 https://www.economist.com/science-and-technology/2019/10/24/lithuanians-are-using-software-to-fight-back-against-fake-news

118. Lietuvos Respublikos Prezidentas, “Fight against Disinformation is EU priority“, Press service, 2019-03-22: https://www.lrp.lt/en/press-centre/press-releases/fight-against-disinformation-is-eu-priority/32098

119. BBC, “I was a Macedonian fake news writer”, Simon Oxenham, 9th May 2019: https://www.bbc.com/future/article/20190528-i-was-a-macedonian-fake-news-writer

120. How Data Privacy Laws Can Fight Fake News, Alex Campbell, 15/08/2019, https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/

121. World Health Organisation. “Vaccine misinformation: statement by WHO Director-General on Facebook and Instagram”, 4 September 2019, Geneva: https://www.who.int/news-room/detail/04-09-2019-vaccine-misinformation-statement-by-who-director-general-on-facebook-and-instagram

123. Europe Is Ready for Its Own Army, 05/09/2019: https://foreignpolicy.com/2019/09/05/europe-is-ready-for-its-own-army/

124. Foreign Policy, “Germany’s Online Crackdowns Inspire the World’s Dictators“ Jacob Mchangama and Joelle Fiss, 6 November 2019: https://foreignpolicy.com/2019/11/06/germany-online-crackdowns-inspired-the-worlds-dictators-russia-venezuela-india/

125. Foreign Policy, “Europe is Ready for Its Own Army”, Azeem Ibrahim, 5 September 2019: https://foreignpolicy.com/2019/09/05/europe-is-ready-for-its-own-army/

126. LRT. “More fake news target NATO’s presence in Lithuania”, 2019-09-27: https://www.lrt.lt/en/news-in-english/19/1101632/more-fake-news-target-nato-s-presence-in-lithuania

127. The Website Poynter index all national measures against Disinformation : https://www.poynter.org/ifcn/anti-misinformation-actions/

128. https://newinform.com/173870-v-sovfede-zayavili-chto-litvu-porazila-totalnaya-rusofobiya

129. Online Infringement: Canadian "Notice and Notice" vs US "Notice and Takedown", 27 June 2012: http://www.entertainmentmedialawsignal.com/online-infringement-canadian-notice-and-notice-vs-us-notice-and-takedown

130. « Manque de moyens, surcharge... les déficits criants de la justice française », Jean-Baptiste Jacquin, 4 October 2018, Le Monde : https://www.lemonde.fr/police-justice/article/2018/10/04/manque-de-moyens-surcharge-les-deficits-criants-de-la-justice-francaise_5364483_1653578.html

131. Foreign Affairs, "Why Putin took Crimea – The Gambler in the Kremlin" by Daniel Treisman, May/June 2016, https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-russian-president-putin-took-crimea-from-ukraine

132. EUvsDisinfo, "Lithuania is afflicted by total russophobia", 13/05/2019: https://euvsdisinfo.eu/report/lithuania-is-struck-by-total-russophobia/

Other Resources

133. Online Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/fake-news

134. Ministère de la Justice, « L'affaire Dreyfus », 23 August 2011: http://www.justice.gouv.fr/histoire-et-patrimoine-10050/proces-historiques-10411/laffaire-dreyfus-22696.html

135. European Parliament News, "Questions and Answers on issues about the digital copyright directive", Press Releases, 27-03-2019: https://www.europarl.europa.eu/news/en/press-room/20190111IPR23225/questions-and-answers-on-issues-about-the-digital-copyright-directive

136. EEAS Website: https://eeas.europa.eu/headquarters/headquarters-homepage_en

137. French President Macron, Discours de la Sorbonne, https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique

138. EUvsDisinfo Website: https://euvsdisinfo.eu/

139. Senat, Dossier Législatif, Loi contre la manipulation de l'information : http://www.senat.fr/dossier-legislatif/ppl17-623.html

140. Website of the European Commission

141. PESCO Website: https://pesco.europa.eu/

142. "Global Alliance for Responsible Media launches to address digital safety", 18 June 2019, World Federation of Advertisers: https://wfanet.org/knowledge/item/2019/06/18/Global-Alliance-for-Responsible-Media-launches-to-address-digital-safety

143. Senator Hawley Introduces Legislation to Amend Section 230 Immunity for Big Tech Companies: https://www.hawley.senate.gov/senator-hawley-introduces-legislation-amend-section-230-immunity-big-tech-companies
and https://www.hawley.senate.gov/sites/default/files/2019-06/Ending-Support-Internet-Censorship-Act-Bill-Text.pdf

144. Political Guidelines for the Next European Commission 2019-2024: A Union that strives for more, My agenda for Europe, By candidate for President of the European Commission Ursula von der Leyen:
https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

145. ECHR Factsheet – Hate speech, October 2019:
https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf

ABSTRACT

The dissemination of false information represents today a major challenge, not because of the novelty of the phenomenon, but because of the novelty of its reach and consequences on the State security and integrity. This research aims at analysing the best ways to fight the phenomenon of spreading false information, by understanding what it is and analysing if there a systematically uniform attitude of the different Member States of the European Union to counter it and if not, whether the European Union can step in. For this purpose, a first part established the characteristics of the phenomenon of disseminating false information and determine the best terminology to reflect properly the phenomenon. The second part elaborates on the possibility of a State to use the principle of State integrity to block foreign content (online or broadcast) while respecting the freedom of expression and the relevant case law of the European Court of Human Rights. Three different legislations – French, German and Lithuanian – are compared in order to determine if they have a uniform and efficient approach and to examine their compliance with the ECHR. Finally, the third part analyse the possibility and opportunity of a European Union approach, by assessing the existing legal framework. The main finding is that the European Union should establish a common framework regarding the definition and responsibility of the platform providers in order to tackle efficiently the dissemination of intended false information, as the national approaches are insufficient and may impair the digital single market.

Keywords: Disinformation – Freedom of Expression – State Security – Broadcast Services

SUMMARY:

The term fake news has become viral in the last few years, especially after the American elections of 2016. Even if the phenomenon of spreading false information is not new - Experts dated it back to 480 BC - it took recently a new extent and resurrected the interest on this matter. The substance of the phenomenon (spreading false or misleading information to influence public opinion) is the same, but its extent is far more alarming. The new means to distribute false information are global, direct and without regulations. It affects all the spheres of society, but States are not measuring yet the consequences and are still lacking a strong will to regulate the phenomenon. After the results of the American elections, experts and governments realised the necessity to understand this phenomenon. This research aims to analyse the best ways to tackle the phenomenon of spreading false information, by understanding what it is and analysing if there is a systematically uniform attitude of the different Member States of the EU to counter it, in respect of the European fundamental rights, and if not, whether the EU can step in.

The first part of the research will therefore focus on the characteristics of false information to determine the best terminology to use, in order to reflect properly the phenomenon.

These clarifications will be used in the second part to compare the national legislations of three selected European States (Lithuania, Germany and France). These States tried to find a balance between the respect of freedom of expression and the necessity to tackle disinformation by blocking foreign content (online or broadcasted). The lack of a common approach and efficiency of those national legislations, and the existence of a competence of the European Union, partly exercised regarding the internal market and audio-visual contents, disclose, the possibility and opportunity of a EU approach.

The major findings are addressed in the third part. Firstly, the European Union should adopt a revision of the e-commerce Directive, to adjust to the major changes of Internet, especially regarding the definition and responsibility of the platform providers. Secondly, even if the self-regulatory approach have proven some good results, it is for now not sufficient and should be complemented, either by an authority in charge of enforcing the self-commitments of the platform, either by an enforceable regulation taken at the EU level in order to ensure more transparency and neutrality regarding the algorithms and the paid advertising.