RSC 2024/19
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

WORKING PAPER

The DSA and the Fight against Online Disinformation in the Context of EU Law: Avenues for Internal Dialogue and External Territorial Extension

Miguel Del Moral Sánchez

European University Institute
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

The DSA and the Fight against Online Disinformation in the Context of EU Law: Avenues for Internal Dialogue and External Territorial Extension

Miguel Del Moral Sánchez

RSC Working Paper 2024/19

ISSN 1028-3625

Published in June 2024 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy

With the support of the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Robert Schumann Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS) was created in 1992 and is currently directed by Professor Erik Jones, and it aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics. The RSCAS is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

Centre for a Digital Society

The Centre for a Digital Society (CDS) was created in 2022 and is directed by Prof. Pier Luigi Parcu. It analyses the chal-lenges of digital transformation and its impact on markets and democracy. Within the EUI, the CDS is part of the Rob-ert Schuman Centre for Advanced Studies. With its research, policy debates and executive training programmes, the CDS aims to advise policy makers on how to cope with the challenges that are generated by the digitalisation process. To do so, it adopts an inter-disciplinary approach, relying on in-house expertise in law, economics and political sciences, and by actively cooperating with computer scientists and engineers from partner institutions.

For further information: https:// digitalsociety.eui.eu/

Abstract

The purpose of this paper is to address the study of the EU rules regarding disinformation, with special emphasis on the DSA and the impact it is set to have both internally, on the legal order of the European Union, and externally, vis-à-vis companies outside the Union. To that end, this article will address, in a first part, the various definitions found in the European context of disinformation, so that this problem and its main elements can be conceptualised. The second part will present the main regulatory instruments that existed before the DSA in this area, the changes brought by the DSA and its main rules to fight disinformation, as well as the possible avenues of judicial dialogue between the CJEU and national courts in this area facilitated by the Regulation and the consequences of the territorial extension of its rules.

Keywords

disinformation, DSA, digital regulation, freedom of expression, judicial dialogue, territorial extension

Table of contents

Introduction

Today, human beings are surrounded by information. This can generate very positive dynamics, allowing access to knowledge to people who would traditionally have been excluded from it and diversifying the sources of information. Online platforms and, notably, social media, have contributed decisively to this trend in recent years. However, this situation has also created what some authors call an 'information disorder',[1] increasing the difficulty of distinguishing truth from lies, facts from opinions, and generating confusion around this information.

Moreover, the algorithms and techniques used by these platforms have favoured the flourishing and dissemination of large amounts of disinformation[2]. Some authors note that this phenomenon is present in all fields, 'from medicine to politics'.[3] The issue of disinformation has drawn a lot of attention throughout the last few years. In Europe, this preoccupation has been fuelled by the evidence of its impact on the Brexit referendum,[4] the information regarding the Covid-19 pandemic,[5] and the Russian war in Ukraine,[6] among others. This has spurred a vast amount of literature that has sought to analyse this issue from multiple perspectives, from the conditions that favour its dissemination[7] to the underpinning structures where it develops.[8] Outside our borders, this situation has also been at the centre of public debate[9].

Disinformation is, first and foremost, a problem of fundamental rights and democracy,[10] as it jeopardises the conditions for citizens to exercise their fundamental right to freedom of expression and damages the pillars of deliberative democracy.[11] But also, it is a problem of regulatory strategy. Some Member States ('MS') have attempted to regulate this phenomenon from different perspectives,[12] raising concerns about undue intrusions into fundamental rights.[13] On the other hand, at the EU level, certain instruments have traditionally acted as firewalls against this phenomenon, notably

1 Claire Wardle and Hossein Derakhshan, 'Information Disorder. Toward an interdisciplinary framework for research and policymaking' (Report DGI(2017)09, Council of Europe 2017) <https://rm.coe.int/0900001680%2076299d> accessed 10 September 2023; Irene Khan, 'Disinformation and freedom of opinion and expression. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (A/HRC/47/25, Human Rights Council 2021) < https://www.ohchr.org/en/documents/thematic-reports/ahrc4725-disinformation-and-freedom-opinion-and-expression-report> accessed 10 January 2024, 2.

2 Ibid 50; Judit Bayer et al. (2019), 'Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States' (European Parliament, LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs 2019), 58; Samantha Lai, 'Data misuse and disinformation: Technology and the 2022 elections' (Brookings 2022) <https://www.brookings.edu/articles/data-misuse-and-disinformation-technology-and-the-2022-elections/> accessed 11 January 2024.

3 Manny Cohen, 'Fake news and manipulated data, the new GDPR, and the future of information' (2017) 34(2) Business Information Review 81, 82.

4 Hannah Marshall and Alena Drieschova, 'Post-Truth Politics in the UK's Brexit Referendum' (2018) 26(3) New Perspectives 89, 95.

5 Oguz Güner, 'From Pandemic to Infodemic: The European Union's Fight Against Disinformation' in Erman Akıllı and Burak Gunes (eds), *World Politics in the Age of Uncertainty* (Palgrave McMillan 2023), 205.

6 Andrew E. Kramer, 'Disinformation is a weapon regularly deployed in Russia's war in Ukraine' *The New York Times* (New York, 26 September 2023) <https://www.nytimes.com/2023/09/26/world/europe/ukraine-russia-war-disinformation.html> accessed 4 January 2024.

7 Natascha A. Karlova, and Karen E. Fisher, 'A social diffusion model of misinformation and disinformation for understanding human information behaviour Information Research' (2013) 18(1) Information Research <https://informationr.net/ir/18-1/paper573.html> accessed 25 October 2023; Gizem Ceylan, Ian A. Anderson and Wendy Wood, 'Sharing of misinformation is habitual, not just lazy or biased' (2023) 120(4) PNAS 1.

8 Johan Farkas and Jannick Schou, 'Fake News as a Floating Signifier: Hegemony, Antagonism and the Politics of Falsehood' (2018) 25(3) Javnost - The Public 298.

9 In the context of the US, see for example Ibid; Craig Silverman, 'Most Americans Who See Fake News Believe It, New Survey Says' *Buzzfeed News* (New York, 7 December 2016) < https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook> accessed 4 January 2023.

10 Khan (n 1) 2.

11 Aysegul Fistikci, 'Démocratie et réseaux sociaux : de la nécessité de la régulation à ses limites' (2023) 21 Cahiers de la recherche sur les droits fondamentaux 29, 33.

12 Ronan Ó Fathaigh, Natali Helberger and Naomi Appelman, 'The perils of legally defining disinformation' (2021) 10(4) Internet Policy Review 1, 8.

13 Csaba Győry, 'Fighting Fake News or Fighting Inconvenient Truths?' (*VerfBlog*, 11 April 2020) <https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/> accessed 9 January 2024; Fotios Spyropoulos, 'Η διασπορά ψευδών ειδήσεων στην εποχή των "fake news"' (*Crime Times*, January 2023) <https://www.crimetimes.gr/η-διασπορά-ψευδών-ειδήσεων-στην-εποχή/> accessed 9 January 2024.

the General Data Protection Regulation.[14] The recent introduction of the Digital Services Act[15] may change much of the current situation, creating the tools and mechanisms to act more decisively against disinformation.

Several authors have analysed some of the rules that tackle this issue at the EU[16] and MS[17] levels. However, given the novel character of the DSA, few scholars have thoroughly studied its obligations, especially in the context of other legal rules with which this Regulation is called to coexist. Most notably, the literature has not addressed yet some of the consequences that the interaction of the DSA with other norms, especially national laws, can bring about in the field of disinformation, as well as the external consequences of its broad scope of application.

In this context, the aim of this paper is to analyse how disinformation is regulated in the European Union, with a special focus on the role of the DSA in this area, and the implications that this Regulation may have both internally and externally. This paper is structured in two parts. The first part will conceptualise the phenomenon of disinformation (section 1.1) and address the different legal definitions of disinformation, both at the Union (section 1.2) and at the national level (section 1.3). The second part will present some of the EU-wide rules that tackle disinformation (section 2.1), with special attention to the DSA (2.2) and the potential internal and external consequences that this Regulation may bring about (2.3).

1. The struggle to legally define disinformation in the EU

1.1. Preliminary remarks and conceptualisation of the issue

In the European context, some scholars[18] have sought to provide a legal definition of disinformation, but there seems to be no consensus as to what this issue entails. However, legally defining disinformation is important for two main reasons: first, and generally speaking, the broader the definition, the more phenomena will be covered by it, enabling regulatory strategies that cover more behaviours but with the subsequent consequences for freedom of expression. Second, and in the specific context of the EU, because the interaction between the conceptions of disinformation at the Union and the domestic levels can play a key role in how this phenomenon is tackled due to the very nature of EU law. Although it is not the purpose of this paper to contribute to the debate on the legal definition of disinformation, it is crucial to acknowledge the various definitions that can be found in the EU context and to conceptualise its elements to facilitate the object aimed by this study.

It should be clarified at the outset that this paper will use the term disinformation and not fake news for two main reasons. First, from a conceptual point of view, the latter term is too vague to encapsulate the complex phenomenon of disinformation. Second, from a normative perspective, this term has been (mis)used in the last years in the political debate and appropriated with spurious purposes to its actual meaning.[19]

Moreover, most scholars agree in distinguishing disinformation from other neighbouring notions, although this is not always uncontested.[20] In this sense, Wardle and Derakhshan note that disinformation, defined as purposive dissemination of false information with the intention of causing

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJL119/1 (GDPR).

15 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJL277/1 (DSA).

16 See, *inter alia, Bayer et al. (n 2); Ó* Fathaigh, Helberger and Appelman (n 12).

17 See, *inter alia,* Ibid; Fistikci (n 11); Christiana Stilianidou, 'Changes to Article 191 of the penal code risk endangering the right to freedom of expression' (*Govwatch report*, 3 December 2021) <https://govwatch.gr/en/finds/i-allagi-toy-arthroy-191-toy-poinikoy-kodika-kai-oi-kindynoi-gia-tin-eleytheria-tis-ekfrasis/#:~:text=Law%204855%2F2021%20amends%20Article,now%20be%20considered%20as%20criminal> accessed 5 January 2024.

18 Ó Fathaigh, Helberger and Appelman (n 12).

19 Wardle and Derakhsan (n 1); Directorate-General for Communications Networks, *Content and Technology, High Level Expert Group on fake news and online disinformation* (Publications Office of the European Union 2018) 10 (HLEG) [in the context of the EU].

20 Luciano Floridi, 'Understanding epistemic relevance' in Luciano Floridi (ed), *The Philosphy of Information* (OUP 2011), 260.

harm, is part of a broader phenomenon of information disorder[21] together with, and distinct from, malinformation, defined as information that is real but spread with the intention of inflicting harm, and misinformation or information that is false but that does not intend to cause harm.[22]

This paper tackles the issue of online disinformation. Although this phenomenon has been repeatedly present throughout history and is certainly not exclusive to the online atmosphere, what is new are the possibilities offered by an ever-changing Internet and technical capabilities, the number of people reached by these tools, and the systemic challenges that this creates.[23] Besides, it is online disinformation that has cantered much of the debate in the literature as well as the regulatory efforts of the EU.

This part is divided into three sections: the first section will present some of the definitions of disinformation formulated at the EU level. The second will provide some examples of regulatory interventions and definitions by MS. Finally, the third section analyses the shared and discordant elements of these definitions and seeks to ascertain their common ground.

1.2. EU-wide concept of disinformation

The growing importance of disinformation for the EU contrasts with the absence of a unified legal definition,[24] which contributes to diminishing the effectivity of the regulatory strategies aimed at countering it and leads the way for laws that may disproportionately affect fundamental rights.[25]

Some instruments at the EU level define disinformation for policy reasons, but not as a matter of law. The Commission set up the 'High-Level Expert Group on Fake News and Online Disinformation' ('HLEG') in 2018 that had the task of advising on policy initiatives to combat the online dissemination of disinformation[26] and that defined this phenomenon as 'all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit'.[27] Acknowledging this report, the European Commission ('EC') issued a Communication in 2018 that defines disinformation as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm'.[28] In 2020, the EC issued another Communication ('On the European democracy action plan') that, in a very similar vein, defined disinformation as 'false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm'.[29]

More recently, and crucially for the aim of this paper, the DSA, in its Recital 104, in the context of the areas of consideration for the voluntary Codes of Conduct encouraged by the Commission, qualifies under the label of disinformation 'the creation of intentionally inaccurate or misleading information, sometimes with a purpose of obtaining economic gain, which are particularly harmful for vulnerable recipients of the service, such as minors'.[30]

These different definitions are summarised in Table 1, where it can be observed that, although some elements are shared between them (i.e., the actions covered by this phenomenon), others exhibit certain differences that may pose legal issues (i.e., the purpose and the extend of the effects).

21 Wardle and Derakhshan (n 1) 20.
22 Ibid.
23 Khan (n 1) 2; Zach Meyers, 'Will the Digital Services Act save Europe from disinformation?' (CER 2022) <https://www.cer.eu/insights/will-digital-services-act-save-europe-disinformation> accessed 25 September 2023; Lai (n 2).
24 Ó Fathaigh, Helberger and Appelman (n 12) 3.
25 Khan (n 1) 3.
26 HLEG (n 19) 5.
27 Ibid 3.
28 Commission 'Tackling Online Disinformation: A European Approach' (Communication) COM (2018) 236 final, 3-4.
29 Commission 'On the European democracy action plan' (Communication) COM (2020) 790 final, 18.
30 However, recitals have no operative effect, and they are not legally binding. As recognised by the ECJ in Case C-162/97 *Criminal proceedings against Gunnar Nilsson* [1998] ECLI:EU:C:1998:554, para 54 "the preamble to a [Union] act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question". However, they do play a role in the interpretation of the provisions.

Table 1: EU definitions of disinformation

	Falsity of the information	Action	Purpose	Potential effect
DSA	Intentionally inaccurate or misleading information.	Created.	Sometimes with the purpose of obtaining economic gain.	Which are particularly harmful for vulnerable recipients of the service, such as minors.
HLEG	False, inaccurate, or misleading information.	Designed, presented and promoted.	Intentionally cause public harm or for profit.	Cause public harm or for profit (idem as purpose).
European Commission	Verifiably false or misleading information.	Created, presented and disseminated.	For economic gain or to intentionally deceive the public.	May cause public harm.

One common and crucial feature of the three definitions[31] and that is shared by most scholars[32] is the actual or potential causation of public harm defined as one or several public goods that deserve protection. In the literature, some authors identify the harm with the very possibility of misleading,[33] although such an approach would be too broad and fail to assess this issue from the perspective of the systemic risks posed by this phenomenon. Precisely from this perspective, Article 34 of the DSA provides some examples of actual or potential public harms like 'the dissemination of illegal content' and the 'negative effects for the exercise of fundamental rights, (…) on civic discourse and electoral processes, and public security; (…) [and] in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being'.

In a similar vein and complementary to it, the HLEG report defined public harm as the threats 'to democratic political processes and values, which can specifically target a variety of sectors, such as health, science, education, finance and more',[34] and the EC adds those threats to 'policy-making processes as well as public goods', and excludes from the definition 'reporting errors, satire and parody, or clearly identified partisan news and commentary'.[35]

Something, however, more contentious is the purpose of the agent disseminating disinformation. From the HLEG report's definition, it can be inferred that it identifies the goal of the actor to the purpose of causing harm or obtaining a certain profit, while the EC establishes that disinformation is 'created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm'. There is no agreement in the literature either, with some authors considering that it is the intention to mislead that characterises disinformation in relation to other forms of information,[36] and others linking this subjective element to the creation of harmful effects as a distinguishing element towards other forms of information disorders.[37]

31 HLEG (n 19) 10; COM (2018) 236 final (n 28) 4; Recital 104 DSA.
32 Wardle and Derakhshan (n 1) 20; Ó Fathaigh, Helberger and Appelman (n 12) 5.
33 Don Fallis, 'What is Disinformation?' (2015) 63(3) Library Trends 401, 406
34 HLEG (n 19) 10.
35 COM (2018) 236 final (n 28) 4.
36 See among others Fallis (n 33) 406; Kai Shu et al. 'Mining disinformation and fake news: Concepts, methods, and recent advancements' in Kai Shu et al. (eds), *Disinformation, misinformation, and fake news in Social Media Emerging Research Challenges and Opportunities* (Springer 2020), 2; Maria Glenski, Svitlana Volkova and Srijan Kumar, 'User engagement with digital deception' in Kai Shu et al. (eds), *Disinformation, misinformation, and fake news in Social Media Emerging Research Challenges and Opportunities* (Springer 2020), 43.
37 See among others Wardle and Derakhshan (n 1) 20; W Lance Bennett and Steven Livingston, 'The disinformation order: Disruptive

In relation to the latter argument, it seems difficult to link the characterisation of disinformation to the specific desired outcomes of the agent which may vary in time and space and often overlap.[38] Motivations are diverse and, as recognised by the DSA and some scholars, may be, *inter alia*, financial,[39] although political motivations tend to draw a lot of attention in both the EU and global contexts. Russian disinformation campaigns, for instance, spread a large volume of information through multiple channels,[40] not seeking consistency (and much less reality) but rather promptness and continuity[41]. In the US, certain political actors, notably Donald Trump, have been in the spotlight for the advantage taken from disinformation campaigns.[42] As Farkas and Schou note, this shows the importance of disinformation today as a 'much larger hegemonic struggle to define the shape, purpose and modalities of contemporary politics'.[43] But whether these political or financial motivations prove an intention to cause harm seems difficult to ascertain and, especially, to prove. Regarding the argument that the subjective element relates to the intention to mislead, some authors rightfully point out that disinformation may not always have the purpose of misleading *per se*, but rather generate multiple and conflicting pieces of information about a topic in order to confuse or disorientate the public.[44] This is particularly the case of Russian disinformation campaigns that, as exposed by Paul and Matthews, disseminate a large volume of information which, regardless of their non-commitment to the objective reality, cannot be concluded to be always entirely false.[45] This, of course, does not mean that the dissemination of true information is caught under the concept of disinformation.[46] It illustrates, on the contrary, that disinformation campaigns often mix true(-ish) and false information,[47] and that, sometimes, some propaganda models (such as the Russian one), with its lack of commitment to the facts, does not intend to create false beliefs as such, but rather contradictory, confusing ones.[48] Moreover, in other instances, disinformation may be a tool to reinforce implicit biases like pre-acquired sexism, racism or homophobia.[49] The purpose of disinformation in these cases may not be to mislead the interpreter (as the latter is already misled), but rather to take advantage of these prejudices through manipulative information.[50] An account of disinformation that relies on the intention purely to mislead seems therefore to be too narrow.[51]

Recital 104 of the DSA seems to support a nuanced version of this latter view. By defining disinformation as 'the creation of intentionally inaccurate or misleading information (…)', it seems to consider that the intention is relevant here to distinguish purposive misleading or inaccurate information from accidental forms of it, rather than for the personal motivations of the actor.

In sum, it could be said that, in the EU, disinformation is defined by an objective element, the risk which is nuclear for the characterisation of this phenomenon, and a subjective one, which relates to the intentionality of the actor that the information she/heis sharing is misleading or deceiving, allowing the distinction of intentional deception or inaccuracies from unintentional instances. The concept of misleading or deceiving must be, however, broadly interpreted to cover the whole range of behaviours and techniques used by these actors.

communication and the decline of democratic institutions' (2018) 33(2) European Journal of Communication 122, 124; Keith Raymond Harris, 'Beyond Belief: On Disinformation and Manipulation' (2023) Erkenn 1, 11.

38 Broadband Commission research report on 'Freedom of Expression and Addressing Disinformation on the Internet', *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression* (International Telecommunication Union 2020), 25.

39 Wardle and Derakhshan (n 1) 34; Fistikci (n 11) 34.

40 Paul Christopher and Miriam Matthews, 'The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It' (2016), Santa Monica, CA: RAND Corporation 1 <https://www.rand.org/pubs/perspectives/PE198.html>, 2.

41 Ibid 4.

42 Farkas and Schou (n 8) 306.

43 Ibid 300.

44 Wardle and Derakhshan (n 1) 30; Harris (n 37) 7.

45 Christopher and Matthews (n 40) 5

46 It would be, in any case, malinformation.

47 Kate Starbird 'Disinformation's spread: bots, trolls and all of us' (2019) 571 Nature 449, 449.

48 Ibid.

49 Cohen (n 3) 82; Lai (n 2).

50 Harris (n 37) 10.

51 Ibid 7.

1.3. National definitions

This phenomenon has not only been addressed at the EU level. As pointed out by many scholars, there has been an increasing tendency by MS to approve laws that regulate disinformation from different perspectives[52] and that define the issue in different ways. Common to these MS laws is that they illegalise (or sometimes criminalise) some forms of disinformation. The divergences in the illegal character of disinformation among MS, as will be later explained in this paper, are likely to provoke several problems due to the interactive nature of EU law. What is relevant at this stage is that, contrary to what is commonly believed,[53] disinformation cannot be concluded to be legal by default in the EU. It will depend on the country, and as this paper will show later on, the DSA could accelerate judicial dialogue in this regard. Although it goes beyond the scope of this paper to thoroughly analyse these national rules, some of them will be briefly presented in this section to show the divergencies in the definition and the illegal nature of some disinformation-related issues. These laws can be divided between those that illegalise some forms of disinformation generally and those that do it in specific times, notably elections or emergency periods.

Examples of both techniques can be found in France. Article 27 of France's Law of 29 July 1881 on Freedom of the Press,[54] which regulates this issue from the point of view of such fundamental right, punishes the 'publication, dissemination or reproduction, by any means whatsoever, of false news or material that has been fabricated, falsified or falsely attributed to third parties when, in bad faith, it has disturbed the public peace or is likely to do so'. The reading of this article allows the action of public authorities with an anticipative nature.[55] Moreover, Law nº 2018-1202, of 22 December 2018, on the Fight Against the Manipulation of Information, criticised by some scholars,[56] defined disinformation, in the specific context of the electoral period, as 'inaccurate or misleading allegations or imputations of a fact likely to affect the fairness of the forthcoming ballot are deliberately, artificially or automatically disseminated on a massive scale via an online public communication service'.[57] It also enables judges, at the request of the 'public prosecutor, any candidate, any political party or grouping or any person with an interest in bringing an action' to order necessary and proportionate measures to cease such dissemination during the three months prior to a general election.

Some examples of other general prohibitions can be found in Greece, Lithuania and Slovakia as well. Greece's Penal Code prohibits, under Article 191,[58] the public or online creation and dissemination of 'fake news that may provoke anxiety or fear in citizens, or shake citizens' trust in the national economy, defence capabilities or public health'. As for the EU definitions, it is the risk, and not the result, that becomes nuclear to the definition of disinformation.[59] However, unlike them, the Greek law criminalises such behaviour, raising questions as to whether this may be an excessive restriction of fundamental rights.[60] Lithuania's Law on the Provision of Information to the Public establishes an 'explicit statutory prohibition on disinformation',[61] defining this phenomenon as 'intentionally disseminated false information',[62] and prohibiting 'to disseminate disinformation and information which is slanderous and offensive to a person or which degrades his honour and dignity'.[63] As a final example, Slovakia prohibits in its Criminal Code (Section 361) the intentional causation of 'a risk of serious concern among at least a portion of the population in a certain location

52 Bayer et al. (n 2) 97; Roxana Radu, 'Fighting the "Infodemic": Legal Responses to COVID-19 Disinformation' (2020) Social Media + Society 1, 2; Ó Fathaigh, Helberger and Appelman (n 12) 8.
53 Ó Fathaigh, Helberger and Appelman (n 12) 2; Annu Bradford, *Digital Empires*, *The Global Battle to Regulate Technology* (OUP 2023), 120.
54 As modified by Article 3 of Order no. 2000-916 of 19 September 2000.
55 Fistikci (n 11) 37.
56 Diane de Bellescize, 'Fake news : une loi polémique, qui pose plus de questions qu'elle n'en résout' (2018) Constitutions 559; Pierre Blanquet, 'La police des fausses informations à l'ère du numérique' (2021) 1 Revue du droit public 149.
57 Article L163-2 of the Electoral Code as modified by 1 of Law 2018-1202.
58 As modified by Article 36 Law 4855/2021.
59 Stilianidou (n 17).
60 Spyropoulos (n 13).
61 Ó Fathaigh, Helberger and Appelman (n 12) 8.
62 Article 2.13.
63 Article 19.2.

by the spread of alarming news, which is false' and the reporting of 'the alarming news or other similar conduct referred to in Subsection 1 to a legal entity or the Police Force or another public authority or mass information facility, even though they know that it is false and may cause a measure leading to serious concern'.

Moreover, some disinformation-related laws that prohibit some of its forms in specific times can be found, among others, in Austria or Hungary. Similar to France in what relates to the election period, Austria's Criminal Code penalises, under Article 264.1, the dissemination of 'false information about a circumstance which is likely to deter persons entitled to vote from voting or to induce them to exercise their right to vote or to vote in a particular way at a time when a counterstatement can no longer be effectively disseminated', although, as recognised by Golla, its scope is relatively limited, given the strong link to the election period that is required.[64] Finally, Section 337(1) of Hungary's Criminal Code criminalises 'claiming or spreading a falsehood or claiming or spreading a distorted fact before a large public, which is suitable for alarming or agitating a large group of people at the site of a public emergency'. An aggravated form is added by section (2), which makes an offence the claim or spread of 'a falsehood or a distorted truth before a large public during an emergency legal regime in a way that is suitable for obstructing or preventing the successful defence'. Nevertheless, as pointed out by Győry, the determination of whether such dissemination is suitable for attaining what required by Section 337(2) 'can only be [done] retrospectively' and is 'inevitably subjective'[65] which, together with the ambiguous character of the definitions provided by this Article, raises problems regarding its compatibility with fundamental rights.[66]

These examples illustrate that different approaches are followed depending on the objectives of each law, not allowing for a unified definition of what behaviours are permitted or prohibited online in the EU, and therefore leaving a rather fragmented environment.

2. Rules to tackle disinformation under the DSA: past, present and future

2.1. Past: the situation before the DSA

Before addressing the study of the new rules introduced by the DSA in relation to the fight against disinformation, it is important to recognise a series of previous instruments that have played (and continue to play) a fundamental role in this area.[67] Two of the most important legal acts, for the aim of this paper, are the E-Commerce Directive[68] and the GDPR, although some others will be briefly presented for the sake of completeness.

The ECD establishes certain provisions in relation to electronic commerce and aims at creating a level-playing field for online services within the EU. Some of its rules have had an undeniable impact in the area of disinformation, notably the liability exemptions (today contained and upgraded in the DSA[69]) of Articles 12-14, the prohibition of Article 15 and the rules related to advertising.[70]

These liability exemptions establish the circumstances under which online service providers are not held liable for the content or information provided by the user of their services. In particular,

64 Sebastian J. Golla, 'Fake-Strafrecht in Wahlkampfzeiten' (*VerfBlog*, 7 September 2021) <https://verfassungsblog.de/fake-strafrecht-in-wahlkampfzeiten/> accessed 9 January 2024.
65 Győry (n 13).
66 Ibid.
67 Van Hoboken et al., 'The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising' (Report for the Ministry of the Interior and Kingdom Relations, 2019).
68 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 **[2000] OJL178/1 (ECD or E-Commerce Directive).**
69 Martin Husovec and Irene Roche Laguna, 'Digital Services Act: A Short Primer' (2022) SSRN <https://ssrn.com/abstract=4153796> accessed 25 September 2023, 3.
70 Van Hoboken et al. (n 67) 57.

hosting services[71] are not liable if they do 'not have actual knowledge of illegal activity or information' or, after 'obtaining such knowledge (…), acts expeditiously to remove or to disable access to the information'. This model is based on the willingness to promote fundamental rights, especially freedom of speech, and an innovative online atmosphere.[72] In the case *Google France,*[73] the ECJ clarified that, for hosting services not to be held liable, it was crucial that their conduct in relation to the information provided by users in them was 'merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which [they] store'[74]. Parallelly, Article 15 ECD establishes the prohibition for MS to create a general obligation to monitor the information transmitted or stored by online service providers. However, scholars pointed out that the ECD did not create the correct incentives for platforms to carry out an appropriate oversee of online activities,[75] often leading to over-removing content generated by their users for staying under the safe harbour and with little attention to freedom of expression.[76] Notably, it was a system that did not provide any safeguard for users whose content was removed. Another provision relevant to the field of disinformation is contained in Article 6 ECD, related to the information that has to be provided in case of commercial communications through online services. The ECD establishes that the commercial communication, the advertiser and the offer have to be 'clearly identifiable as such'.

In sum, the ECD has played an important role in tackling disinformation through the creation of a system where online service providers (information society services, in the language of the Directive) must take down illegal content upon knowledge of it being hosted by them, and where commercial communications, and the person sponsoring it, is recognisable. The former is important to tackle disinformation, but it is only related to content that is illegal and, although some MS have illegalised certain types of disinformation, it is not always the case. As established before, the illegality or not of the content is not a feature of disinformation in the EU. The latter provides some transparency as to who is behind advertising on platforms, although only for commercial communications.

Moreover, data protection has traditionally been the most important legal field for tackling disinformation. It enjoys constitutional protection in the EU, guaranteed by Article 8 of the Charter, and is mainly codified in the GDPR. As exposed previously, a big part of disinformation is transmitted by profiling techniques facilitated by the use of data.[77] The algorithms of online platforms are fed with large volumes of user data in order to target them with content that they are likely to interact with. As discussed above, the risks this creates in relation to misinformation relate not only to confirmation bias and the creation of echo chambers,[78] but also to the potential manipulation and confusion of users. Under the GDPR, any processing of users' data must be done 'lawfully, fairly and in a transparent manner', for 'specified, explicit and legitimate purposes', and 'adequate, relevant and limited to what is necessary', among others (Article 5(1) GDPR).

In 2019, the European Data Protection Board issued a statement (Statement 2/2019) in relation to the use of data for political campaigns where the risks posed by the profiling techniques in these situations were highlighted. It reminded the special character of data related to political opinions (Article 9(1) GDPR) and that, as such, there is a prohibition by principle of their treatment save for when 'explicit, specific, fully informed, and freely given consent of the individuals'[79] has been given.

71 This paper focuses on hosting services, defined by the ECD as an "information society service (...) that consists of the storage of information provided by a recipient of the service" (Article 14(1)). The reason is that it is through this kind of services that illegal and harmful content is ultimately transmitted (as recognised, among others, by Recital 50 DSA). This definition is also contained in Article 6 DSA, under the label of which online platforms like social and content-sharing platforms, online marketplaces, and app stores are among others covered.

72 Caio C.V. Machado and Thaís Helena Aguiar, 'Emerging Regulations on Content Moderation and Misinformation Policies of Online Media Platforms: Accommodating the Duty of Care into Intermediary Liability Models' (2023) 8 Business and Human Rights Journal 244.

73 Joint Cases C-236/08 to 238/08 [2010] ECLI:EU:C:2010:159.

74 Ibid, para 113.

75 Yassine Lefouili and Leonardo Madio, 'The Economics of Platform Liability' (2022) 52 European Journnal of Law and Economics 319, 343.

76 Van Hoboken et al. (n 67) 59.

77 Lai (n 2).

78 Wardle and Derakhshan (n 1) 50; Bayer et al. (n 2) 58.

79 Point 1 Opinion 2/2019 EDPB in relation to Article 9(2) GDPR.

These safeguards apply as well to other data related to characteristics such as racial or ethnic origin, health, sex life or sexual orientation, trade union membership, etc. As pointed out by Van Hoboken et al., the GDPR is a key tool to prevent disinformation campaigns as, without prejudicing the lawfulness of the content itself, establishes several safeguards for targeting the audience by using their data.[80]

Naturally, outside the aforementioned categories, users' data is still protected, and the latest developments of the case law in data protection can contribute even further to a safer, GDPR-compliant atmosphere and, subsequently, to raise walls against disinformation campaigns. In the case *Österreichische Post AG,*[81] the Austrian Postal Service was using data related to several socio-demographic criteria from citizens and selling it to several organisations which then sent them targeted publicity.[82] The data collected was not specifically linked to political orientation but allowed the Austrian Post to infer the political affinity of the data subjects,[83] and the person in the main proceedings claimed that '[t]he fact that data relating to his supposed political opinions were retained within that company caused him great upset, a loss of confidence and a feeling of exposure', which should justify a non-material damage compensation of 1000€ on the basis of Article 82 GDPR. In its judgement, the ECJ interpreted the concept of 'damage', and more specifically, of 'non-material damage' as an autonomous notion of EU law[84] which does not reach any specific threshold of seriousness for giving rise to compensation.[85] By ruling out a *de minimis rule in damage compensation,*[86] this judgement opens the door, on the one hand, to the empowerment of users vis-à-vis companies through immaterial damages. This is especially relevant in the online atmosphere, where the damage suffered by every specific individual is usually very small, but the cumulation of those damages can have systemic consequences.[87] Through the piecemeal aggregation of small individual infringements, companies astronomically increase their profits at the expense of creating significant social harm. Non-material damages, and their broad interpretation by the ECJ in *Österreichische Post,* are thus likely to help shifting the balance of power for the benefit of users and to empower them to claim restitution in case of unlawful uses of their personal data. Moreover, it can have a preventive effect, incentivising online companies to be more attentive concerning GDPR compliance and, by the same token, acting as a firewall against disinformation.

Apart from the ECD and the GDPR, some other rules have played a more modest but still relevant role in the regulatory framework against disinformation. The rules of the Audiovisual Media Services Directive[88] apply to video-sharing platforms[89] with the idea that online intermediaries have a certain degree of control over the content shared in them, especially in relation to the way it is enabled or ranked within the platform.[90] The AMSD seeks to protect 'minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development', as well as the general public from user-generated videos and audiovisual commercial communications that incite violence or with certain offences under EU law (Article 28b(1)). It seeks to ensure that audiovisual commercial communications are, among others, 'recognisable as such' and prohibiting 'surreptitious audiovisual communications' and 'subliminal techniques' (Article 9(1)(a) and (b)), but without leading to ex-ante monitoring which does not comply with the E-Commerce Directive (Article 28b(2)¶2). Moreover, Article 28b(3) establishes certain measures that MS shall apply, as appropriate, for the purposes of video-sharing platforms complying with the rules of the

80 Van Hoboken et al (n 67) 60.
81 C-300/21 [2023] ECLI:EU:C:2023:370.
82 Ibid, para 11.
83 Ibid, para 12.
84 Ibid, para 45.
85 Ibid, para 46.
86 Shu Li, 'Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21' (2023) Maastricht Journal of European and Comparative Law 1 (note).
87 Stephan Mulders, 'The relationship between the principle of effectiveness under Article 47 CFR and the concept of damages under Article 82 GDPR' (2023) 13(3) International Data Privacy Law 169, 169.
88 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2010] OJL95/1 (AMSD or Audiovisual Media Services Directive).
89 Article 1(aa).
90 Van Hoboken et al. (n 67) 64.

AMSD. Although Article 1(h) does not include political advertisement from the concept of audiovisual commercial communications, Van Hoboken et al. note that Article 28b also covers 'user-generated videos' that could well include 'campaign videos and videos containing political communication uploaded by a political party or group'.[91] The AMSD creates another defensive wall to prevent disinformation in online video-sharing platforms through certain rules that tackle the content generated by users and commercial communications posted in them. Other norms, such as the e-Privacy Directive[92] and the Unfair Commercial Practices Directive[93] have been recognised by some scholars to play a role in this area as well[94].

2.2. Present: disinformation-related rules under the DSA

As pointed out in Part 2, no instrument at the EU level defines disinformation with legal effects, i.e., there is no harmonisation of this notion in the Union. Some of those instruments, such as the DSA, provide for definitions only for regulatory policy reasons, and the teleological analysis of some of its articles. It is under this perspective that the rules contained in the DSA regarding disinformation have to be analysed; with Recital 104 in mind, the risk caused by disinformation is, as advanced before, central to the definition of this phenomenon. For that reason, many of its rules, especially those directed towards Very Large Online Platforms or Search Engines (VLOPs/VLOSEs), focus on risk assessments and mitigation measures.

Before plunging into the novelties brought about by the DSA, mention should be made to the EU Code of Practice on Disinformation of 2018 and its reform of 2022. The Code of 2018 established a number of compromises for the signatory companies in order to tackle disinformation and was 'the first such (government-encouraged) self-regulatory initiative in the world'.[95] Interestingly, the Code of Practice of 2018 already introduced a differentiated approach in the application of the compromises according to the size and capabilities of companies, something that is present in the architecture of the DSA. However, as pointed out by scholars the Code of 2018 failed to meet its expectations[96]. The 'Sounding Board' created for assessing the Code noted the lack of a 'common approach, (…) clear and meaningful commitments, (…) measurable objectives (…), possibility to monitor process', and acknowledged the absence of a 'compliance or enforcement tool'.[97] More worryingly, the report stated that this instrument was 'by no means self-regulation, and therefore the Platforms, despite their efforts, have not delivered a Code of Practice'.[98] Moreover, the Commission itself recognised that the Code had several shortcomings and issued a Communication in 2021[99] that resulted in the Code of Practice of 2022. The Communication of 2021 pointed out that the drafting of the new Code was intended to transform it into a 'Code of Conduct' under the meaning of the DSA, allowing signatories to anticipate compliance to the obligations that will later apply under the still-being-drafted Regulation.[100]

91 Ibid 66.
92 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJL201/37.
93 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] L149/22.
94 Van Hoboken et al. (n 67) 67.
95 Peter H. Chase, 'The EU Code of Practice on Disinformation: The Difficulty of Regulating a Nebulous Problem' (2019) TWG on Content Moderation Online and Freedom of Expression <https://www.ivir.nl/publicaties/download/EU_Code_Practice_Disinformation_Aug_2019.pdf> accessed 3 December 202, 5.
96 Ibid 11; Joris Van Hoboken and Ronan Ó Fathaigh, 'Regulating Disinformation in Europe: Implications for Speech and Regulating Disinformation in Europe: Implications for Speech and Privacy' (2021) 6 UC Irvine Journal of International, Transnational, and Comparative Law 9, 15.
97 The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice (24 September 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54456> accessed 28 November 2023, point 3.
98 Ibid.
99 COM (2021) 262 final.
100 Ibid 3.

The Strengthened Code of Practice of 2022 builds on the experience of the Code of 2018 and explicitly recognises itself as a Code of Conduct in the sense of Article 45 DSA.[101] It does not mean that the companies subject to the DSA will forcibly and automatically be subject to the Code of 2022. The Code of 2022 must be read in conjunction with the DSA. The former is a voluntary set of rules that complements the latter binding instrument which aims at regulating the conduct of online intermediaries.[102] However, as recognised by Recital 104 of the DSA, adhering to it is recognised as an 'appropriate risk mitigating measure' (in the meaning of Article 35 DSA) and, in case of 'refusal without proper explanations (…) of the Commission's invitation to participate in the application of such a code of conduct could be taken into account (…)' to assess non-compliance by a company of their obligations under the DSA.[103] Yet, mere participation in the Code does not account for automatic compliance with the Regulation.[104] By the end of 2023, the signatories of this Code are companies like TikTok, Microsoft, Meta, and Google, among others. There are notable absences like Twitter (now X) which abandoned the Code in May 2023.

Although some authors consider self-regulation as the most efficient way to counter the potential market failures of the online sector,[105] the literature often points out the problems in terms of enforcement[106] and the short-term, profit-oriented incentives that may play against the eagerness of certain firms to pursue self-regulation.[107] The model established by the DSA is one of co-regulation, where the interaction between the regulator and the regulated platforms will be paramount for its success. The Code of 2022 is an example of this idea.[108]

Moving to the DSA itself, it must be pointed out at the outset that, although the fight against disinformation is clearly one of the targets of the DSA, there is no specific set of rules created exclusively to that effect. Conversely, several provisions of the Regulation address this issue from multiple perspectives and can be categorised into liability rules, content-related rules, and transparency and risk mitigation rules.

Liability rules of the DSA

The DSA maintains the liability exemptions and content-moderation principles of the ECD and upgrades them.[109] Thus, under Articles 6 DSA, online hosting intermediaries continue to avoid liability for the content stored by their users as long as they do not 'have actual knowledge of illegal activity or illegal content' or 'upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content'. Moreover, Article 7 DSA states that voluntary own-initiative investigations carried out by intermediaries in order to detect and remove illegal content, or in relation to other obligations provided for by EU law in general and the DSA in particular, shall not provoke the loss of the liability exemption.[110] These rules reaffirm and uphold the liability exemptions of the ECD, as well as the prohibition of imposing general monitoring set down in Article 15. As pointed out before in the context of the E-Commerce Directive, they can help to tackle disinformation as they provide incentives to put down illegal information shared in online service providers as soon as they have knowledge of it and allows users to flag such content.

101 2022 Strengthened Code of Practice on Disinformation, 2.
102 Mark Leiser, 'Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation' (2023) SSRN <https://ssrn.com/abstract=4427493> accessed 12 September 2023, 8.
103 Recital 104 DSA.
104 Recital 104 DSA.
105 Molly Cohen and Arun Sundararajan, 'Self-Regulation and Innovation in the Peer-to-Peer Sharing Economy' (2017) 82(1) University of Chicago Law Review 116, 132.
106 Pieter Nooren et al., 'Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options' (2018) Policy & Internet 264, 285.
107 Michael A Cusumano, Annabelle Gawer and David B Yoffie, 'Can self-regulation save digital platforms?' (2021) 30(5) Industrial and Corporate Change 1259, 1288.
108 Code of Conduct 2022, 2.
109 Husovec and Roche Laguna (n 69) 3; Leiser (n 102) 4.
110 The so-called "Good Samaritan clause".

Rules to tackle illegal content

The so-called 'due diligence obligations' are the real innovation brought about by the DSA and complement the liability exemption regime[111] which was very fragmented and had failed to fully solve the issues of disinformation and protection of the freedom of expression.[112] This new approach based on a 'duty to care' by online companies was anticipated in 2017 by the German Netzwerkdurchsetzungsgesetz (NetzDG) and introduced at the EU level with the DSA.[113] In a similar vein to the Codes of Practice against Disinformation of 2018 and 2022, the DSA establishes an asymmetric, incremental regime, whereby the obligations imposed on online service providers increase according to their size.

Among these rules, those related to the detection and elimination of illegal content are very relevant in the context of disinformation. As pointed out before, although at the EU level there might be a conception that disinformation should not, in principle, be illegal, this is not the case in several MS. Many have passed laws making unlawful, sometimes even criminalising, certain types of disinformation. Therefore, any analysis of the DSA's approach towards this phenomenon cannot overlook the role of the 'notice-and-action mechanisms' of Article 16-17 (applicable to all hosting services), and 'trusted flaggers' of Article 22 (applicable to online platforms).

As a preliminary note, it must be reminded that the DSA does not set or harmonise the rules in relation to which content or behaviour is illegal,[114] which is a competence of MS. In the field of disinformation, this is very likely to create 'soft conflicts' triggered by the divergent, opposing approaches of MS in relation to the legality of certain types of content,[115] which may lead to different enforcement depending on the country, but that will certainly provoke that the mechanisms designed to flag and take down illegal content will be applicable to this phenomenon in certain MS.

The notice-and-action mechanism obliges hosting services to put in place mechanisms that allow users to flag the presence of illegal content in an 'easy to access and user-friendly' fashion (Article 16(1) DSA), leading to the consideration that the platform has 'actual knowledge or awareness' in the sense of Article 6 of the DSA.[116] Additionally, Article 17 DSA establishes an obligation to provide a 'clear and specific statement of reasons to any affected recipients of the service' in case of restriction of their content.

Moreover, the DSA creates the so-called 'trusted flaggers', defined as 'entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content and that they work in a diligent, accurate and objective manner'[117] and that are designated by the MS' Digital Service Coordinator.[118] According to Article 22(1) DSA, notices submitted by them must be given priority and decided without undue delays.

In MS where certain types of disinformation are considered illegal, these mechanisms will play a crucial role in tackling this phenomenon. In fact, it is in these countries where the DSA will have a greater impact in the fight against disinformation, not without the potential concerns for freedom of expression. Users and trusted flaggers will be able to notice any content that they believe is illegal under their national laws and, for online platforms to avoid liability, it will have to be taken down expeditiously, limiting its impact and dissemination.

111 Husovec and Roche Laguna (n 69) 4.
112 Machado and Aguiar (n 72) 248.
113 Ibid 249.
114 Husovec and Roche Laguna (n 69) 11.
115 Ibid.
116 Article 16(3) DSA.
117 Recital 61 DSA.
118 Article 22(2) DSA.

Non-illegal-content-related obligations

When it comes to content that is not illegal but that is nonetheless harmful to society or groups of it, there are several obligations imposed by the DSA on online intermediaries that can play a very important role.

The 'online interface design and organisation' obligations of Article 25 are very important in this regard, prohibiting online platforms from designing, organizing or operating 'their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions'. The guidelines on the application of this Article will clarify its extent, but what seems undeniable is that it is called to facilitate free choice by users in the online environment and prevent them from being deceived by the platforms.

Advertising obligations of Article 26 DSA also upgrade the provisions of the ECD, especially Article 6, and Article 28b and 9 of the AMSD on commercial communications, by harmonising the information that must be made available for platforms to present advertisements on their services (e.g., the fact that it is an advertisement or who is behind it or who is paying for it). The main difference with the ECD and the ASMD, and that is of paramount importance for fighting against disinformation, is that 'advertisement' is defined by Article 3(r) of the DSA as 'information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes and presented by an online platform on its online interface against remuneration specifically for promoting that information', therefore potentially including also political advertisement. And crucially as well, paragraph 3 of Article 26 prohibits, without exceptions, the targeting of individuals for advertisements of any type based on the special categories of data of Article 9(1) of the GDPR.[119] Thus, one of the biggest drivers of disinformation, i.e., micro-targeting, is very restricted by the DSA. Connected to it, Article 28(2) prohibits the targeting of minors with any personal data whatsoever for the purposes of advertisement. As clear as the harmful effects of these practices of certain online platforms, there were no clear and homogeneous rules in this regard at the EU level before.

Transparency and risk mitigation rules

The literature has pointed out the lack of transparency as one of the biggest stones in the way to tackle disinformation.[120] It is precisely in this field, together with risk mitigation, where scholars seem to agree that the DSA has made one of its greatest contributions.[121]

Article 15 establishes the obligation for all online intermediaries to provide reports concerning the moderation of content that they carry on. Moreover, Article 24 poses additional transparency reporting obligations for online platforms 'in view of their particular responsibilities and obligations'.[122] These platforms are also subject to the obligation of Article 27, concerning recommender systems transparency. This is crucial as well in the context of disinformation, as recognised by Recital 70 DSA, given the key role of recommender systems in the dissemination of certain messages and behaviours online, and increasing transparency and information in this domain is crucial for enhancing users' self-determination over the content they see and share. Besides, given the 'additional risks relating to their activities and their additional obligations under [the DSA]',[123] Articles 39 and 42 impose further transparency obligations for VLOPs/VLOSEs, the former in relation to online advertising in their platform, and the latter to reporting obligations.

119 Especially sensitive data.
120 Wardle and Derakhshan (n 1) 80; HLEG (n 19) 22; Bayer et al. (n 2) 12; Van Hoboken and Ó Fathaigh, (n 96) 16.
121 Meyers (n 23) 2; Leiser (n 102) 5.
122 Recital 65.
123 Recital 100.

Given that VLOPs/VLOSEs are deemed to pose the highest risks concerning disinformation,[124] they are subject, under the DSA, to an additional set of due diligence obligations to the assessment and mitigation of those risks. Article 34 obliges those platforms to 'diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services'. They must therefore conduct risk assessments in relation, among others (and especially relevant in the context of disinformation), to systemic risks such as 'dissemination of illegal content', or 'actual or foreseeable negative effects' on 'fundamental rights' and 'civic discourse and electoral processes, and public security', considering the gravity of the potential consequences and the probability of these risks.[125] In this context, Recitals 80-83 provide some guidance on the assessment of the aforementioned risks.

The need for current or potential risks created by these platforms to be systemic aligns the DSA's assessment and mitigation mechanisms with the European-level policy definitions of disinformation, where social harm is identified in 'function of the relationship between the qualitative assessment of the risk posed by the content in context and a quantitative measure of the reach and/or intensity of exposure of audiences to that content'.[126] To that effect, such assessments need to take into account whether and how these systemic risks are spurred by the 'design of their recommender system and any other relevant algorithmic system; their content moderation systems; the applicable terms and conditions and their enforcement; systems for selecting and presenting advertisements; [and] data related practices of the provider', as well as by 'intentional manipulation of their service, including by inauthentic use or automated exploitation of the service'.[127]

Based on these assessments, Article 35 DSA mandates that VLOPs/VLOSEs must proportionately and effectively mitigate such risks, with special attention to fundamental rights. The measures deriving from this obligation are varied and may include the adaptation of the architecture of the platforms' systems, their terms and conditions, certain content moderation techniques, the adjustment of the advertising systems, etc.[128] As recognised by Article 35(3), these measures will require future guidelines by the Commission to ensure a certain degree of consistency, legal security and respect for fundamental rights.

In addition to these mechanisms, the DSA also contains certain rules about crisis management. Particularly, Article 36 creates a crisis response mechanism that allows the Commission, in case of a crisis,[129] to require VLOPs to take certain actions if the functioning of their systems is posing a serious threat.[130] The introduction of the mechanism of Article 36 came, after the 3rd trialogue of the DSA, as a consequence of the Russian invasion of Ukraine, and raised some rule of law concerns given the powers granted to the Commission in this field.[131] Moreover, Article 48 establishes the voluntary crisis protocols that can help the coordination of Union-level responses, among others, to situations 'where online platforms are misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information'.[132]

Before moving to the expected internal and external legal outcomes derived from these rules, it is important to note that, in 2021, a proposal for a Regulation on the transparency and targeting of

124 Recital 100; Leiser (n 102) 4-5.
125 Recital 79.
126 Directorate-General for Communications Networks, Content and Technology, *Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns* (Publications Office of the European Union 2023) 15 (DG Connect).
127 Article 34(2) DSA.
128 In line with DG Connect (n 126) 23.
129 Defined as "extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it" (Article 36(2) DSA).
130 For further analysis of this Article, see Doris Buijs and Ilaria Buri, 'The DSA's crisis approach: crisis response mechanism and crisis protocols' (*DSA Observatory*, 21 February 2023) <https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/> accessed 10 January 2024.
131 EDRi, 'On New Crisis Response Mechanism And Other Last Minute Additions To The DSA' (Public Statement, 2022) <https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/> accessed 10 September 2023; Ibid.
132 Recital 108.

political advertising[133] was launched, and in November 2023, an agreement was reached between the co-legislators on its text. In its Recital 4, the proposal recognises the key role of political advertisement for the dissemination of disinformation, and the centrality of transparency for the achievement of the goals of Article 2 TEU. In that spirit, it harmonises the rules regarding 'transparency obligations for providers of political advertising and related services to retain, disclose and publish information connected to the provision of such services' and on 'the use of targeting and amplification techniques in the context of the publication, dissemination or promotion of political advertising that involve the use of personal data'.[134] Importantly, and in a similar vein as the DSA and the GDPR, the proposal establishes a broad territorial scope, covering any political advertising 'prepared, promoted, published or disseminated in the Union', irrespectively of where the service provider is established and the means used.[135] This Regulation will play a key role in enhancing transparency of what content shared in platforms is political and who is behind it, although concerns have been raised by some scholars in the very broad definition of political advertisement,[136] affecting not only political actors but also any message 'which is liable to influence the outcome of an election'.[137] It also creates a notice-and-action mechanism for users to flag the content that does not respect its rules. Although it falls outside the scope of this paper to analyse the potential ways of interaction between the DSA and the proposed Regulation, it is crucial to recognise that their future interactions will be key in the EU's regulatory strategy to counter disinformation.

2.3. Future: Judicial Dialogue and Territorial Extension

After discussing the articles of the DSA that will play a key role in targeting disinformation, this section aims to analyse the potential outcomes derived from their interaction with the EU and national legal systems, both internally and externally.

2.3.1. Illegality of disinformation and judicial dialogue

The existing literature has paid little attention to the lack of substantive harmonisation in relation to illegal content. Although some authors have pointed out the potential conflicts between the laws of MS[138] or those resulting from EU private international law,[139] the question of the interplay between the DSA's rules and national laws from the point of view of judicial dialogue has not been addressed yet.

This article has echoed the existing legal literature's remark that many MS have illegalised certain types of disinformation, at least in specific periods like elections or during events of crisis,[140] provoking a deep fragmentation within the EU on what behaviours are permitted both off and online. From the online service providers' perspective, this is highly problematic, as they will continue to be subject to 27 different legal frameworks for the provision of their transnational services, with the legal uncertainty this situation may create. Although this is a logical consequence of the primarily procedural focus of the DSA[141] and may be seen as a reasonable burden in exchange for the benefits derived from their presence in multiple markets,[142] there is no doubt that it seems, first and foremost, inconsistent with the DSA's goal as an internal market instrument of 'provid[ing] businesses with access to new markets and opportunities to exploit the benefits of the internal market, while allowing

133 COM (2021) 731 final.
134 Article 1(1) of the Proposal.
135 Article 1(2) of the Proposal.
136 Max van Drunen et al., 'The EU is going too far with political advertising!' (*DSA Observatory,* 16 March 2023) <https://dsa-observatory.eu/2023/03/16/the-eu-is-going-too-far-with-political-advertising/> accessed 10 September 2023.
137 Article 1(2)(b) of the Proposal.
138 Husovec and Roche Laguna (n 69) 11.
139 Tobias Lutzi, 'The Scope of the Digital Services Act and Digital Markets Act: Thoughts on the Conflict of Laws' (2023) Dalloz IP/IT, 4 (forthcoming).
140 Bayer et al. (n 2) 97; Radu (n 52) 2; Ó Fathaigh, Helberger and Appelman (n 12) 8.
141 Pietro Ortolani, 'If You Build it, They Will Come. The DSA "Procedure Before Substance" Approach' in Joris van Hoboken et al. (eds), *Putting the DSA into Practice* (Verfassungsbooks 2023), 154; Miguel del Moral Sánchez, 'The Devil is in the Process: Private Enforcement in the DMA and the DSA' (2024) 9(1) University of Bologna Law Review (forthcoming), 47.
142 Pedro De Miguel Asensio, *Conflict of Laws and the Internet* (Edward Elgar 2020), 8.

consumers and other recipients of the services to have increased choice'[143] and 'safeguard[ing] and improv[ing] the functioning of the internal market [through] a targeted set of uniform, effective and proportionate mandatory rules'.[144]

More importantly, however, the resulting scenario after the introduction of the DSA can have a very crucial impact on the subject matter of disinformation from the viewpoint of the potential judicial dialogue between domestic courts and the ECJ with regards to national laws that regulate certain aspects of the freedom of expression. Even if there is some truth in the claim that the DSA puts 'procedure before substance',[145] in the sense that it lays down a number of due diligence and redress obligations for online service providers instead of focusing on regulating the content transmitted by them,[146] two caveats should be bore in mind. First, as pointed out by some scholars, the link between the rights conferred to individuals and the procedural remedies available for their redress is very narrow, making them often undistinguishable[147]. As noted by Tridimas, 'it may not be possible to separate the redress requested from the underlying right whose protection is sought'.[148] Second, the very wording of the DSA seems to underline the interaction between the general principles and fundamental rights of EU law and the regulation of digital services, not only from a procedural but also from a substantive point of view.

In the context of the DSA and disinformation, the distinction between the procedural and substantive side of the right to freedom of expression and information is hard to assess. For example, the rules on notice-and-action mechanisms aim at safeguarding the fundamental rights of the affected parties as guaranteed by the Charter, including freedom of expression.[149] But as fundamental-rights-compliant as the procedure established by the DSA to take down the allegedly illegal content may be, it could not, without violating Article 11 of the Charter, uphold national rules that by themselves violate the substance of this right. As much as a compliant substantive interference with this right would not be capable of compensating for a defaulting procedure, the same should be true the other way around.

Furthermore, in its Recitals, the DSA recognises that some of the rules adopted by MS that jeopardise the functioning of the Internal Market, and that consequently fall under its scope, relate to the handling of illegal content.[150] Indeed, although Recital 9 recognises that MS are able to maintain national rules applicable to intermediary service providers when they do not fall under the scope of the Regulation, it also states that such rules must nevertheless comply with EU law. It also upholds the importance of the rights laid down in the Charter, among which the freedom of expression and information of Article 11.[151] When it comes to the definition of illegal content, it is true that the DSA has a very broad approach,[152] referring to the domestic laws of MS, giving them the competence to establish the substantive rules on this matter.[153] However, Article 3(h), echoed by Recital 12, refers to the 'law of any Member State which is in compliance with Union law', thus considering that national rules on illegal content that are activated under the provisions of the DSA should as well comply with the whole architecture of Union law, and most importantly with the Charter. This conclusion is further supported by Article 9, which sets some minimum conditions that the orders issued by national authorities to online service providers must comply with.[154] Article 9(2)(ii) thus requires 'a statement of reasons explaining why the information is illegal content, by reference to one or more specific provisions of Union law or national law *in compliance with Union law'.* Moreover, *Recital 32* further clarifies that '[t]he applicable national law should be in compliance with Union law, including the Charter'.

143 Recital 2.
144 Recital 4.
145 Ortolani (n 141) 162.
146 Ibid 154.
147 Walter Van Gerven, 'Of Rights, Remedies and Procedures' (2000) 37 CML Rev 501, 525.
148 Takis Tridimas, 'Financial regulation and private law remedies: an EU law perspective' in Olha O. Cherednychenko (ed), *Financial Regulation and Civil Liability in European Law* (Edward Elgar 2020), 48.
149 Recital 52.
150 Recital 2.
151 Recital 3.
152 Recital 12.
153 Article 3(h) and Recital 12.
154 Recital 31.

Therefore, it may be more accurate to say that the DSA, more than just putting procedure before substance, creates a harmonised procedure for national substantive rules, both of them, however, falling under the scope of EU law. In other words, by establishing an EU procedure for taking down illegal online content, the DSA elevates national rules that regulate such content, among which those that illegalise certain types of disinformation, to the EU level, with the derived obligation that they must comply with Union law, including the Charter.

It is relevant at this point to briefly acknowledge the approach of the ECJ and the ECtHR towards freedom of expression, with particular emphasis on the field of disinformation. The right to freedom of expression is guaranteed by Article 11 of the Charter, the meaning and scope of which corresponds to the one of Article 10 of the ECHR, as provided by Article 52(3) of the Charter. Both Courts consider this right to be at the very basis of a working democratic society[155] and one of the core values of the European Union.[156]

The ECtHR has not so far directly tackled disinformation in its judgements, although some of them address some issues connected to it.[157] In its judgement *Brzeziński v. Poland*[158] *of 2019*, it was the first time the ECtHR mentioned the term 'fake news', something that was criticized by many scholars given that it was not raised by any of the parties and the controversial nature of the term.[159] Moreover, the Strasbourg Court has recognised both the positive[160] and the pernicious[161] consequences that the online environment may have for the enjoyment of fundamental rights.[162] Notably, the ECtHR has highlighted the importance of the reach of a publication online in order to determine its potential influence.[163]

In its landmark case *Handyside v. UK of 1976*, the ECtHR already pointed out that the right of Article 10 protects both information or ideas which are considered favourable or inoffensive and those that actually 'offend, shock or disturb'.[164] Moreover, in its case *Salov v. Ukraine of 2005*, the Strasbourg Court noted that:

> Article 10 of the Convention as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful. To suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media and would thus place an unreasonable restriction.[165]

The ECtHR distinguishes between facts and value judgements, providing for higher protection to the latter, which are, according to the Strasbourg Court, 'not susceptible of proof',[166] showing a particular preoccupation with the harmful effects of falsity in the presentation of facts,[167] and pathing the way for potential regulatory interventions by States Parties in this regard. There is also a crucial distinction between political and non-political forms of expression in the jurisprudence of the ECtHR, with higher protection provided for the former.[168] However, such a dichotomy is not clear in the context of disinformation as political and commercial communications usually intertwine and are part of the same phenomenon.[169]

155 *Handyside v UK* App no 5494/72 (ECtHR, 7 December 1976), para 49.
156 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016] ECLI:EU:C:2016:970, para 93.
157 Sofia Verza, 'Case law for policy making: an overview of ECtHR principles when countering disinformation' (Project number SMART 2019/1087, European Digital Media Observatory 2020), 4.
158 App no 1781/13 (ECtHR, 4 February 2014).
159 Ibid 4; Davor Muhvić and Ivana Rešetar Čulo, '"Fake News" in Times of Crisis in the Context of Article 10 of the European Convention on Human Rights' (2022) 43(1) Zbornik Pravnog fakulteta Sveučilišta u Rijeci 189, 196.
160 *Cengiz and Others v. Turkey* App nos 48226/10 and 14027/11 (ECtHR, 29 March 2016).
161 *Editorial Board of PravoyeDelo and Shtekel v. Ukraine* App no 33014/05, 5 May 2011).
162 Verza (n 157) 5.
163 *Savva Terentyev v. Russia* App no 10692/09 (ECtHR, 28 August 2018), para. 79.
164 *Handyside v UK* (n 155), para 49.
165 App no 65518/01 (ECtHR, 27 April 2004), para 113.
166 *Lingens v Austria* App no 9815/82 (ECtHR, 8 July 1986), para 46.
167 Muhvić and Rešetar Čulo (n 159) 201.
168 *Lingens v Austria* (n 166), para 42.
169 See, for example, the issues raised in the case *Mouvement Raëlien Suisse v Switzerland* App no 16354/06 (ECtHR 13 July 2012).

Naturally, the right to freedom of expression is not absolute, and there are certain instances where it can be limited by other conflicting interests. Art 10(2) ECHR establishes that this right is accompanied by certain 'duties and responsibilities' that justify limitations when 'prescribed by law and (…) necessary in a democratic society (…)'. Equally, Article 52 of the Charter permits the limitation of fundamental rights 'provided for by law', respecting 'the essence of those rights and freedoms', 'subject to the principle of proportionality' and 'only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

Although it goes beyond the scope of this paper to analyse whether national laws illegalising certain forms of disinformation comply with these conditions, it seems clear that the system created by the DSA opens the door to their scrutiny by the ECJ through Article 263 TFEU. The cooperative nature of the preliminary reference procedure makes it a key tool for the judicial dialogue between the ECJ and national courts,[170] and can play a very important role in the field of disinformation by leading MS to put aside certain national laws that are deemed incompatible with EU law, achieving some degree of similarity in the outer limits of this phenomenon.

2.3.2. Territorial extension of the DSA

The term 'territorial extension' seems the most accurate to explain the global reach the DSA's rules are likely to have. Scott refers to the territorial extension of a norm or a measure when its application depends on circumstances or behaviours that occur outside the EU but that still have a territorial connection with the territory of the Union.[171] The global reach of EU legislation has been highlighted by several authors,[172] and while extraterritorial rules, purely conceived, are still very unusual in its legal order, the Union uses far-reaching territorial connections that have profound effects outside its borders.[173] This phenomenon has special importance concerning Internet-related activities, the nature of which fosters the territorial expansion of certain EU rules.[174] Precisely in this relation, the existing literature agrees that the scope of the GDPR leads to the clear territorial extension of its rules[175] given that it applies to 'the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.[176] The GDPR has several avenues for the territorial expansion of its rules, from its scope of application to the rules related to data transfers to countries outside the EU.[177]

In the field of disinformation, such territorial extension seems crucial for the fulfilment of the objectives of any regulatory intervention. Disinformation is a global phenomenon that is very often prompted or facilitated by companies outside the EU. If the rules that tackle this phenomenon had a geographical scope restricted to European companies only, they would be incapable of having profound effects. It seems clear that, together with the GDPR, the DSA also has a territorial scope that allows for its application to conduct that take place outside the borders of the EU.[178] This philosophy is embedded in the very nature of the Regulation, which recognises that the effectiveness of its norms depends on such broad territorial connection[179] and is materialised into Article 2(1), which states that the DSA 'appl[ies] to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those

170 Takis Tridimas, 'The ECJ and the National Courts: Dialogue, Cooperation, and Instability' in Damian Chalmers and Anthony Arnull (eds), *The Oxford Handbook of European Union* Law (OUP 2015), 407.
171 Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2013) 62(1) The American Journal of Comparative Law 87, 90.
172 Ibid 88; Merlin Görmann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 CML Rev 567, 578; Annu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020), 17.
173 Scott, 'Extraterritoriality and Territorial Extension in EU Law' (n 171) 94.
174 Cedric Ryngaert, and Mistale Taylor, 'The GDPR as Global Data Protection Regulation?' (2020) 114 AJIL Unbound 114 5, 5.
175 Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2019), 124; Ibid 6; Bradford, *The Brussels Effect* (n 172) 131.
176 Article 3(1) GDPR.
177 Kuner (n 175) 124.
178 Laureline Lemoine, 'The extraterritorial implications of the Digital Services Act' (*DSA Observatory, 1 November 2023)* <https://dsa-observatory.eu/2023/11/01/the-extraterritorial-implications-of-the-digital-services-act/> accessed 15 December 2023.
179 Recital 7.

intermediary services have their place of establishment'. Scholars agree that these practices form part of a broader policy of the Union that seeks to alter the global behaviour of firms and exercise its global regulatory power.[180] As pointed out by Anu Bradford, the EU seeks to uphold its values and conception of digital regulation outside its own borders,[181] where the protection of the preconditions for citizens to exercise their freedom of expression plays a key role.[182] A regulatory intervention that seeks to counter disinformation with a human-centric and fundamental rights-based approach, where the protection of individual, political and collective rights are ensured, is the cornerstone of this policy,[183] and the DSA is embedded of this logic. The broad territorial scope of this Regulation seeks to ensure that companies that want to access the Union's market, and obtain benefits therefrom, comply with its regulatory requirements.

While the DSA rules clearly give rise to territorial extension because they require to take into account the conduct of companies that may not be established in the EU, this is not directly translated into the possibility of them having a strong 'Brussels Effect'. This theory was developed by Anu Bradford and refers to 'the EU's unilateral ability to regulate the global marketplace'[184] and has given rise to a rich literature concerning several EU instruments. The Brussels Effect can be *de facto*, where companies change their global behaviour to comply with EU rules, or de jure, where third countries modify their own rules in line with the European ones.[185] Bradford also points out five conditions under which the Brussels Effect is likely to occur, i.e. 'market size, regulatory capacity, stringent standards, inelastic targets, and non-divisibility'.[186] Without entering into the discussion of the specificities of these elements, it should be noted that, while the first two relate to the EU itself, the last three are specific to the rule in every case. Besides, while rules that give rise to a territorial extension may foster the presence of some of these elements, it does not necessarily result in the unilateral regulatory globalisation of such rules.[187]

Some scholars agree that European data privacy in general, and the GDPR in particular, is a clear example of both territorial extension and Brussels Effect,[188] and some even qualified it as 'unashamedly global'.[189] Whether this will be the case for the DSA and, particularly for the aim of this paper, for its disinformation-related rules, will depend especially on the last two elements identified by Bradford, namely the inelasticity of the target and the lack of divisibility. Article 2 of the DSA, with its territorial scope similar to the one of the GDPR, favours such inelasticity, as it avoids the possibility of the delocalisation of companies to less stringent countries. The latter, however, deserves further discussion. As noted by Bradford, the non-divisibility of standards can be economic, technical and legal.[190] It seems clear that some of the disinformation-related rules of the DSA make it very difficult, or even impossible, to create differentiated rules for the provision of services within and outside the EU, or at least generate very high incentives for companies to find more beneficial to apply EU rules for their global conduct. For example, although risk assessment and mitigation obligations mandate VLOPs to 'analyse and assess any systemic risks in the Union', the factors that have to be taken into account and the measures that must be put in place as a result of such assessment include features related to the very design of these platforms that make it very difficult or costly to divide.[191]

180 Scott, 'Extraterritoriality and Territorial Extension in EU Law' (n 158) 106; Bradford, *The Brussels Effect* (n 172) 10.
181 Bradford, *Digital Empires* (n 53) 105.
182 Ibid 119.
183 Ibid 121.
184 Bradford, *The Brussels Effect* (n 172) 1.
185 Ibid 2.
186 Ibid 25.
187 Joanne Scott, 'The Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2019), 32.
188 Görmann (n 172) 568; Ryangaert and Taylor (n 174) 9; Bradford, *The Brussels Effect* (n 172) 131.
189 Duncan Robinson, 'EU removes carrot but keeps stick in data laws' *Financial Times* (London, 20 January 2016) <https://www.ft.com/content/9d774734-a4b1-11e5-a91e-162b86790c58> accessed 10 December 2023.
190 Bradford, *The Brussels Effect* (n 172) 55.
191 For example, the adaptation of the design, features and functioning or content moderation policies of the platform's service, or the modification of the algorithms or recommender systems (Article 35(1) DSA).

Moreover, the level at which the phenomenon of territorial extension takes place will be particularly relevant[192] as it can spur the legal non-divisibility of the standards. As noted by Scott, there are three types of territorial extension: transaction-level, firm-level and country-level.[193] The clearest example of firm-level territorial extension of disinformation-related that is likely to foster the Brussels Effect is the non-deception by design obligation of Article 25 that mingles with the ex-ante design of service providers, irrespective of whether there is a potential systemic risk or not.

These few examples illustrate how the rules related to disinformation contained in the DSA are likely to have a key impact on the global regulatory atmosphere of this phenomenon. While the existence of a Brussels Effect that would lead companies to adapt their global conduct to the EU rules (and, potentially, third countries to modify their own norms) is still unlikely and will depend on many factors, it seems clear that the broad territorial scope of the DSA will oblige foreign companies to comply with its burdensome rules. Such territorial extension shows how the EU is 'using market access as a tool to leverage the migration of its frequently demanding norms abroad'.[194]

Conclusion

This paper has shown that the regulatory strategy against disinformation in the European Union is very fragmented, both horizontally (with diverse norms that tackle this phenomenon from different perspectives) and vertically (as both the Union and its MS are issuing norms that target it). The DSA has been one of the last pieces in this puzzle and, together with the GDPR, is one of the instruments that is likely to revolutionise the most the regulatory atmosphere of the online environment.

It is important to note, as shown before, that the dichotomy between illegal and harmful content for defining disinformation cannot be upheld. Especially because several MS have issued rules that illegalise (and sometimes even criminalise) certain forms of disinformation, either in general or in specific periods (i.e., elections or times of crisis). The legality of disinformation will depend on its specific content and the MS where it occurs.

As argued by this article, it is difficult to acknowledge a single definition of disinformation in the EU. Multiple rules or communications establish different elements, and scholars do not seem to agree on any particular one. What seems clear is that most legal definitions agree that disinformation is characterised by a subjective element (the intentionality of the actor) that distinguishes it from unintentional forms of misleading information and an objective one (the risk caused by it). It is precisely around the notion of risk, or systemic risk, that the DSA's rules that deal with disinformation are structured. They do so especially through the transparency rules and the obligations related to risk assessment and mitigation and crisis mechanisms. In a co-regulatory fashion, the DSA makes online service providers (particularly online platforms) active participants for the achievement of a safer, more transparent online atmosphere that respects the rights of users (especially their freedom of expression and information) and favours the necessary conditions for their fulfilment. Additionally, other rules of the DSA are nuclear in this area as well. Given that some countries illegalise certain types of disinformation, all the constellation of norms that relate to illegal content will be relevant in these places as well. The liability exceptions and due diligence obligations like the notice-and-action mechanisms and the trusted flaggers, among others, will play a key role in this domain.

The DSA is also likely to have a both internal and external impact. Internally, it could enhance judicial dialogue between the ECJ and national courts in relation to illegal content and freedom of expression, applying the Charter to situations that now fall under the scope of EU law. Externally, the broad territorial scope of the DSA will provoke the application of its norms to the conduct of foreign companies and can have profound effects on their services and their global behaviours. Potentially, it could enhance the unilateral regulatory power of the European Union through the so-called 'Brussels Effect'. Yet, it should be acknowledged that the DSA is a very recent instrument, and the practice

192 Scott, 'The Global Reach of EU Law' (n 187) 34.
193 Ibid 25-26.
194 Scott, 'Extraterritoriality and Territorial Extension in EU Law' (n 171) 88.

and casuistic will determine the direction it takes, and its effects on disinformation. Moreover, in a field like online regulation, innovations appear every moment, and regulatory interventions, as novel as they can be at the beginning, can very rapidly become obsolete. The capacity of the Union to adapt its norms to both technical and social developments will be paramount for the success of the objective of tackling disinformation and creating a safe and respectful online milieu, centred in the protection of persons and their fundamental rights, and with due regard to allowing for innovation and competition.

Author

Miguel Del Moral Sánchez

Academic Assistant in the Law Department of the College of Europe in Bruges

miguel.del.moral.sanchez@coleurope.eu