

ARTICLE

Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 *Infodemic* and the Feasibility of a Consumer-centric Solution

Ruairí Harrison*

Since 2016, the European Commission has sought to take a proactive stance in addressing disinformation, with this stance evidently influenced by the divisive nature of disinformation and its ability to dissuade participation and trust in democratic institutions. Yet as the coronavirus pandemic brought fear and uncertainty to Europe and the wider world, how well equipped was the Commission's approach for the onslaught of health disinformation which accompanied the pandemic? Reflecting on the EU's soft law approach both before and after this 'Infodemic,' this article critically analyses the inherent difficulties in regulating disinformation and looks ahead to the Commission's proposed approach into the future. Finally, considering these inherent regulatory difficulties and the impact of the Infodemic, this paper reflects upon the feasibility of a 'consumer-centric' solution to tackling disinformation in the European Union.

Keywords: Covid-19; fundamental rights; freedom of expression; Digital Services Act; European Commission; free speech; disinformation; content moderation; digital regulation

1. Introduction

As conversations around the globe concerning the issue of online disinformation gather gravity and frequency, it is tempting to view disinformation as a 21st century problem. Yet disinformation appears to be as old as recorded human conflict, with General Sun Tzu famously noting that 'all warfare is based on deception' in the fifth century BC.¹ Disinformation can also be traced back to Octavian's grappling for power in the turbulent post-Caesar Civil War period. Here, the first Roman Emperor manipulated information concerning his first adversary, Marcus Antonius, using brief rhetorical notes engraved on coins and circulated around Rome. These notes painted his rival as a drunk, a womaniser and a headstrong soldier incapable of ruling an empire.² They ultimately proved their effectiveness in gaining the public's support and their simple, accessible form and message could be compared to a modern day 'Tweet'; for example, Trump declaring the 2020 US presidential elections as fraudulent in a series of easy-to-read tweets devoid of evidence.

Although any comparisons between the outgoing US President and Caesar Augustus may begin and end there, the potency of 21st century digital disinformation is what sets the issue apart from previous incarnations: online disinformation campaigns weaponise the user community to spread swathes of disinformation as fact. Thus, while the campaign may be traced back to, for example, a Kremlin operation, its damage is done by the millions of users spreading such messages as fact. Yet what makes designing a regulatory solution to disinformation so problematic is an inherent conflict. This conflict concerns the importance of promoting free speech online to encourage public debate, for instance on global public health issues such

* This article was written by Ruairí Harrison in his personal capacity and does not represent the views of the European Commission or the Utrecht University School of Law, IE; email: harrisru@tcd.ie.

¹ Sun Tzu, *The Art of War* (Chiron Academic Press, 2015) ch 1, verse 18.

² C. Suetonius Tranquillus, *The Lives of the Twelve Caesars* (Loeb Classic Library, 1913).

as the Covid-19 pandemic, versus the need to regulate disinformation so that public debate on such issues is not ill-informed.

Therefore, the core aims of this article are (i) to analyse critically the EU Commission's response to online disinformation thus far, (ii) to examine the primary solutions proposed by the Commission into the future, and (iii) to assess if any feasible alternative solutions exist to tackle disinformation in the longer term. Each of these core aims will be assessed in light of the role which coronavirus disinformation played in bringing renewed urgency to the problem of disinformation in the EU.

This article will be structured as follows: Section I will frame the issue of disinformation in the EU by discussing its origins, its purposes and the varying types of disinformation affecting the EU at present. Section II will put forth the response of the European Commission (from herein referred to as the 'Commission') to disinformation from 2017 to 2019 alongside a critical analysis of its 2018 Code of Practice on Disinformation. Section III will focus on developments in 2020 surrounding the efficacy of the Commission's response to widespread Covid-19-related disinformation and its impact on online consumers. Section IV analyses the references to disinformation in the EU's Digital Services Act, followed by a discourse on the feasibility of a 'consumer-centric' approach as a long-term solution to disinformation online. Finally, a general conclusion will be offered on the findings of this article.

2. Disinformation in the EU – Framing the Problem

The terms disinformation, misinformation and fake news – often used interchangeably – have never truly left Western public discourse since 2016. This discussion was brought forth by two major events in 2016 on either side of the Atlantic (the Brexit Referendum and the US Presidential Election), both of which will be returned to later. Yet before contextualising disinformation, it is imperative to address inherent definitional challenges as well as its varying types, purposes and its distinction with misinformation.

In brief, the distinction between disinformation and misinformation is the *intent* of the person sharing content. 'Disinformation' is the sharing of false or misleading content with the intent to deceive, whereas 'misinformation' is the sharing of false or misleading content without the intent to mislead (or without knowledge of its falsity).³ This distinction is best illustrated by the following contemporary example:

John sees a post shared by an Anti-Vaxxers page which appears in his Facebook news feed. It is simply a photo with ten sentences of text of information about the Covid-19 vaccines discouraging people from taking it. The post has no sources, and unknown to John, some claims made are verifiably false; thus, this is considered **disinformation**. However, as John is genuinely scared by what he has read, he decides to share the post with his Facebook friends; this is **misinformation**.

In recent years, Commission proposals regarding content moderation have struggled with definitional issues regarding 'terrorist content'⁴ and 'hate speech',⁵ and the associated free speech concerns of overly broad definitions, yet nowhere is this issue as pertinent as with disinformation. As noted by Jason Pielemeier, 'it can be extremely difficult to objectively determine the truth in a given context, much less establish whether an individual knew or should have known that certain information was untrue.'⁶ This uncertainty leaves users prone to self-censorship: '(...) individuals [may] refrain from sharing content (as well as opinions) they perceive as objective or newsworthy but cannot independently or reliably verify.'⁷ Of course, the foundational free speech provision in European democracies, Article 10 of the European Convention on Human Rights, allows for inroads to be carved into the freedom – for instance to regulate commercial expression.⁸ Similarly, the EU legislature has restricted free speech for broader policy reasons as in the 2019 Copyright Directive.⁹ However, the unique position of disinformation as merely 'harmful' content as opposed to 'illegal' prevents the tackling of disinformation from being an easily justifiable restriction on free speech. This 'harmful'

³ Commission, Joint Communication on 'Tackling COVID-19 disinformation - Getting the facts right' JOIN(2020) 8 final.

⁴ Commission, 'Proposal for a Regulation on preventing the dissemination of terrorist content online' COM[2018] 640 final.

⁵ Commission, 'EU Code of Conduct on Countering Illegal Hate Speech' (Brussels, May 2016).

⁶ Jason Pielemeier, 'Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?' (2020) 4 Utah Law Review 917, 922.

⁷ Ibid.

⁸ *Markt intern Verlag-GmbH v Germany*, App No 10572/83 (ECtHR, 20 November 1989), para 35.

⁹ Parliament and Council Directive (EU) 2019/790 of 17 April 2019 on Copyright and Related rights in the Digital Single Market (2019) OJ L 130/92.

vis-à-vis 'illegal' differentiation will be returned to in later sections alongside an explanation of why it has led the Commission to avoid a paternalistic approach where possible, instead emphasising the merits of co-regulation with social media platforms and the empowerment of users to recognise disinformation.

Secondly, the two most problematic 'types' of disinformation which impact the online community in 2021 are 'political' disinformation and 'health' disinformation. 'Political' disinformation is using false or misleading information to further a political end, whereas 'health' disinformation is false or misleading information related to public health matters. The two types may interlink where Covid-19 health disinformation is utilised to promote a political movement which simultaneously uses political disinformation to further its own objectives.¹⁰

Finally, in framing the 'disinformation' issue in the EU, an awareness of the variety of purposes which disinformation can serve ensures that the regulatory response is flexible and multi-layered.

(i) Disinformation can be used by domestic governments to gain or protect political power:

When the 'Vote Leave' campaign infamously spread 'We send the EU £350 million a week, let's fund our NHS instead' on buses during the Brexit referendum, the simplicity of this message was potent, and it was widely circulated online.¹¹ This claim is now accepted by critics and proponents alike as a vast over-simplification which deliberately misled voters.¹²

(ii) Disinformation can be used by domestic governments to hide mistakes or distract its population:

In China, the so-called '50 cent party'¹³ of government sponsored online commentators will post emotive, unrelated comments online in order to provoke audience reactions against the individual commentator who has criticised government action.¹⁴ This diverts the online discourse away from state criticism.¹⁵

(iii) Disinformation can be used by foreign actors to divide and polarise other societies:

The obvious example here is Russian 'meddling' in the 2016 US Presidential Elections. Amongst other techniques, fabricated articles and disinformation were spread from Russian government-controlled media and promoted on US social media.¹⁶ This was done to damage the Clinton campaign, boost Trump's chances and sow distrust in American democracy overall.¹⁷

(iv) Disinformation can be financially lucrative:

Studies have shown that disinformation is widely shared online because it provokes extreme reactions and commands attention from the public; users are more likely to click on links that display content that is extreme, provocative or contentious.¹⁸ Those purposely spreading disinformation are

¹⁰ European External Action Service, 'Pro-kremlin disinformation: Covid-19 Vaccine' (EU Delegation to Azerbaijan, 22 December 2020) <https://eeas.europa.eu/delegations/azerbaijan/90950/pro-kremlin-disinformation-covid-19-vaccines_en> accessed 14 June 2021.

¹¹ 'Vote Leave' Campaign, 'We send the EU £350 million a week - let's fund our NHS instead' (2016) <<https://digital.library.lse.ac.uk/objects/lse:pen598xoz>> accessed 14 June 2021.

¹² Andrew Reid, 'Buses and Breaking Point: Freedom of Expression and the 'Brexit' Campaign' (2019) 22 *Ethical Theory and Moral Practice* 623.

¹³ Samantha Bradshaw, Philip Howard, 'Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation' (University of Oxford: Working Paper, 2017[12]), 8–9.
See also 9 of above: '... "50 Cent Party", so-called because of a rumour that government-sponsored internet commentators were paid 50 cents every time they posted messages online.'

¹⁴ *Ibid.*

¹⁵ European Parliament, 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States' (Policy Department for Citizens' Rights and Constitutional Affairs, DG for Internal Policies of the Union Report [PE 608.864 – February 2019]), 30.

¹⁶ Special Counsel Robert Mueller III, 'Report on the Investigation into Russian Interference in the 2016 Presidential Election' (US Department of Justice, Washington, March 2019 [submitted pursuant to 28 C.F.R. § 600.8(c)]), 4.

¹⁷ *ibid.*, 4.

¹⁸ João Pedro Baptista and Anabela Gradi, 'Understanding Fake News Consumption: A Review' (MDPI, *Soc. Sci.* 2020, 9, 185); (doi: 10.3390/socsci9100185), 1.

not only misleading the public, but they may also ask users for financial support towards the project, as is common in QAnon forums.¹⁹ From the platform's perspective, associated advert revenues are also much higher as misleading posts so often gain more online traction online.²⁰

Each of these purposes and related examples brought into sharp focus the need to take steps to tackle disinformation in the EU. In fact, concerns about Russian disinformation interfering with EU affairs led to the establishment of the East Strategic Communication Task Force in 2015.²¹ Yet it was not until 2016 that a broader statement was made in the European Union Global Strategy (EUGS) regarding the concept of 'resilience' and disinformation being cited as a major threat to European resilience.²² It is to this period of 2017–2019 that we now turn in order to assess the Commission's next steps in meeting this threat to European resilience.

3. The Commission's Response to Disinformation – 2017–2019

3.1. Crafting a Response to Reflect European Values

As above, the turbulent year that was 2016 and the role which *political* disinformation played in events in the UK and US spurred the Commission into further action. The first Commission 'Action Plan' released cites European Council conclusions regarding Russia's use of disinformation in the Salisbury Russian nerve agent attacks,²³ the Syrian War and the downing of the MH-17 aircraft in Ukraine as justifying European '*resilience against hybrid threats*' becoming a priority for further work.²⁴ Yet regarding this malleable concept of 'resilience,' the European Commission had to assess how best to tackle disinformation considering European neoliberal values. On either side of the spectrum of [content] regulation are the paternalistic approach and the adaptive approach.

Firstly, the paternalistic approach is one in which the state takes an interventionist stance in filtering information for public discourse. This approach appears heavy-handed when considering 21st century European values; it would include tackling disinformation by direct state oversight using measures such as propaganda to reshape public discourse or by banning certain persons from publication. Thus, the EU has sought to remain resilient against disinformation threats by predominantly using the softer 'adaptive' approach; this approach 'influences citizens without resorting to measures that could... harm free speech' including media literacy, fact-checking and platform self- and co-regulation.²⁵ Therefore it is evident that neoliberal values allow the Commission to delegate *some* responsibility for addressing disinformation on society:²⁶ the state actor sets local level practices but delegates a limited role to the 'user community.'²⁷

Returning to the primary EU Developments, the 2019 European Parliament Elections became somewhat of a benchmark early on, referenced in the 2018 Action Plan as the next event in which disinformation would pose a potential threat to democratic resilience in the Union.²⁸ The Commission's 'Code of Practice on Disinformation' came into force in October 2018 in lieu of this Action Plan.²⁹ This soft law measure was signed by Facebook, Google, Twitter, Mozilla, and several online advertisers in October 2018 and has more recently been signed by Microsoft (May 2019) and TikTok (June 2020).³⁰ Looking to the substance of the

¹⁹ Brandy Zadrozny, Ben Collins, 'How three conspiracy theorists took 'Q' and sparked Qanon' (NBC News, 14 August 2018) <<https://www.nbcnews.com/tech/tech-news/how-three-conspiracy-theorists-took-q-sparked-qanon-n900531>> accessed 14 June 2021.

²⁰ See Baptista and Gradi (n 18), 14.

²¹ European External Action Service, East StratCom Task Force (Unit): unit was created by the European Council, citing the 'need to challenge Russia's ongoing disinformation campaigns [in Russia and neighbouring countries]' (European Council, 'European Council Meeting Conclusions' (Brussels, 20 March 2015 [OR/en] EUCO-11/15) para 13.

²² European External Action Service, 'Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy' (EUGS, June 2016) <https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf> accessed 14 June 2021, 8.

²³ European Council, 'European Council Meeting Conclusions' (Brussels, 23 March 2018 [OR. En] EUCO 1/18) paras 9–11.

²⁴ Commission, Joint Communication on the 'Action Plan Against Disinformation 2018' JOIN(2018) 36 final, 1.

²⁵ TA Romanova, NI Sokolov, YY Kolotaev 'Disinformation as a Threat to Democratic Resilience: Approaches used in the EU and its Member State Lithuania' (2020) 12 *Baltic Region* 53, 55.

²⁶ David Chandler, Jon Coaffee, 2017, *The Routledge Handbook of International Resilience* (Routledge 2019), 19.

²⁷ See Romanova, Sokolov and Kolotaev (n 25), 56.

²⁸ Commission, Joint Communication on 'Tackling Online Disinformation: A European Approach' (COM[2018] 236 final) para 3.2.

²⁹ Commission, 'EU Code of Practice on Disinformation' (Brussels, October 2018).

³⁰ Commission Website, 'Policy – Code of Practice on Disinformation' (Media Convergence and Social Media Unit I.4, 18 January 2021) <<https://ec.europa.eu/digital-single-market/en/code-practice-disinformation>> accessed 14 June 2021.

Code, 'disinformation' is defined as 'verifiably false or misleading information' which is created for economic gain or to deceive the public, and may cause public harm.³¹ The definition explicitly excludes 'misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary and is without prejudice to [other] binding legal obligations...'³²

The 2018 Code focuses on five core commitments, which are accompanied below by a brief synopsis:³³

- A. Scrutiny of ad placements: firms commit to disrupting the monetisation incentives of disinformation sources by working with fact-checkers.
- B. Political and issue-based advertising: ensure transparency in these forms of advertising by clearly distinguishing such adverts from editorial content; political adverts must be subject to public disclosure.
- C. Integrity of services: clear policies must be put in place regarding the identity and misuse of automated bots on platforms. Signatories must also draft policies on what constitutes 'impermissible use of automated systems' and make these policies publicly available.
- D. Empowering consumers: signatories should invest in technologies which prioritise verified, relevant information and make it easier for people to find diverse perspectives on public interest topics. Efforts must be made to improve *critical thinking and digital media literacy*.³⁴
- E. Empowering the research community: signatories commit to support good faith independent efforts to tackle disinformation, including an EU-wide independent network of fact-checkers. This must include the sharing of privacy protected datasets.³⁵

Finally, the 2018 Code provides 'Key Performance Indicators' (KPIs) to monitor the Code's effectiveness relating specifically to each of the five commitments alongside a statement on the relevant assessment period for the effectiveness of the Code being every 12 months. Yet it is argued that it is just as important to highlight what is *not* included in the Code when assessing the Commission's response to disinformation. For the purposes of clarity, the critical analysis below will focus solely on the pre-Covid-19 pandemic period and is gathered from both academic publications and relevant Commission publications.

3.2. Critical Analysis – Why did the Code Fall Short of Expectations?

To begin, it would be unfair to wholly dismiss the effectiveness of the 2018 Code; several of its features can be seen in a positive light. Firstly, its flexibility encourages platforms to sign up without the fears of over-regulation. Secondly, its soft law nature meant there was no strict, lengthy legislative path – platforms could incorporate the commitments into their Terms of Service immediately. Thirdly, it acknowledged the inherent *borderlessness* of online communication – meaning an EU-wide approach to disinformation regulation is preferable to deviating national approaches. The Code was evidently a step in the right direction, yet it is submitted that the overly cautious nature of this step was insufficient to address such a vast problem.

To begin, the limits of the Commission's soft law powers related to its 'Communications' and associated 'Codes' have been evident for some time. Francis Snyder comments on how the *France v Commission*³⁶ and *ERTA*³⁷ cases ensured a 'Code' should be 'a simple explanatory document' and may not impose legal obligations on member states.³⁸ Unlike EU secondary law, Commission soft law initiatives do not state agreed upon definitions – as is crucial for content moderation. This lack of uniform definitions across the platforms inhibits effective action to fulfil commitments as well as impeding a proper evaluation of the Code's

³¹ See Commission (2018 Code) (n 29), 1: 'public harm' is intended as 'threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security.'

³² See Commission (2018 Code) (n 29), 1 continues: '... binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising.'

³³ *Note*: given the broad nature of this article, the five core commitments will simply be stated and briefly summarised.

³⁴ *Note*: the unique importance of *critical thinking and digital media literacy* as a longer-term solution to online disinformation will be returned to in Section IV of this article.

³⁵ See Commission (2018 Code) (n 29), 4–8.

³⁶ C-303/90 *France v Commission* [1991] ECR I-05315.

³⁷ C-22/70, *Commission v Council* [1971] ECR I-263.

³⁸ Francis Snyder, 'The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques' (1993) 56 Mod L Rev 19, 34–35.

effectiveness.³⁹ The lack of definitional uniformity also heightens concerns about the fundamental rights impacts of privatised enforcement of content moderation; the UN stated that “[g]eneral prohibitions on the dissemination of information based on vague and ambiguous ideas, including “false news” or “non-objective information”, are incompatible with international standards for restrictions on freedom of expression.”⁴⁰

Two other significant issues are presented by the soft, self-regulatory nature of the Code. Firstly, the European Regulators Group for Audiovisual Media (from herein the ‘ERGA’) note how the voluntary nature of the Code establishes a ‘regulatory asymmetry’ between Code signatories and non-signatories.⁴¹ This opens up the possibility of disinformation sources continuing their practices at non-signatory platforms negating much of the progress made by the Code’s signatories. Secondly, the Code’s self-regulatory nature has prevented the establishment of an independent oversight mechanism. Alongside the Code’s promotion of ‘self-assessment’, there is no real means to ascertain the signatories’ compliance with the Code or sanction signatories for Code breaches.

Related to this inherent limitation of ‘self-assessment reporting’ is the fact the Code fails to go far enough regarding the reporting and monitoring obligations, particularly regarding the platforms’ opacity in how content is being monitored. KPIs were seen as necessary to accommodate different business models at the platforms, yet this has led to several varying reporting structures with different monitoring methods; this impedes productive comparative analysis of the Code’s effectiveness.⁴² Related to this, platforms have not been transparent in sharing ‘robust, raw data’ which would help improve understanding of disinformation in the EU across all platforms.⁴³ The ERGA’s report found that the platforms’ reporting only disclosed aggregate EU-level data, which ‘limits the possibilities for a truly independent and objective verification’ of reporting.⁴⁴ The Commission itself found that:

The lack of access to data allowing for an independent evaluation of emerging trends and threats posed by online disinformation, as well as the absence of meaningful KPIs to assess the effectiveness of platforms’ policies to counter the phenomenon, is a fundamental shortcoming of the current Code.⁴⁵

This lack of access to pertinent datasets is also detrimental to the Code’s commitment to ‘empowering the research community.’⁴⁶ More work needs to be done to standardise the ‘quality of the datasets [that] should be made available to the research community at large’ in order to acquire a better understanding of disinformation.⁴⁷

To conclude, it is evident that the 2018 Code took cautious steps in the right direction and succeeded in engaging with platforms in an expedient manner. Yet this hands-off, voluntary approach was also the *Achilles Heel* of the Commission’s approach.⁴⁸ The success of the approach depended heavily on the voluntary cooperation of the signatory platforms: the signatories only had to agree to commitments that they were comfortable with, whilst maintaining an opaque exterior as to how disinformation was being tackled. In brief, this *Achilles Heel* has meant that there is no mechanism to adequately assess Code compliance and no real consequences for non-compliance. Despite this, it is submitted that the delicate balancing act between promoting free forums of public debate and tackling the disinformation which pollutes these

³⁹ Commission, ‘Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement’ SWD(2020) 180 final, 13: for example, “Political advertising”: loosely defined under pillar B of the term has been delineated in varying ways by the platforms themselves and is defined differently at Member State level, or is not defined.

⁴⁰ UNHCR, ‘Joint Declaration on Freedom of Expression and “Fake News,” Disinformation And Propaganda’ (FOM.GAL/3/17, 3rd March 2017) <<https://www.osce.org/files/f/documents/6/8/302796.pdf>> accessed 14 June 2021, 4.

⁴¹ ERGA ‘Report on Disinformation: Assessment of the Implementation of the Code of Practice’ (ERGA, May 2020) <<https://erga-online.eu/wpcontent/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf>> accessed 14 June 2021, 44.

⁴² See Commission (Code Assessment) (n 39), 16.

⁴³ See Commission (Code Assessment) (n 39), 16.

⁴⁴ ERGA, Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation (June 2019) <https://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf> accessed 14 June 2021.

⁴⁵ See Commission (Code Assessment) (n 39), 19.

⁴⁶ See Commission (2018 Code) (n 29), Section II.E.

⁴⁷ See Commission (Code Assessment) (n 39), 11.

⁴⁸ Antonios Kouroutakis, ‘EU Action Plan Against Disinformation: Public Authorities, Platforms and the People’ (The International Lawyer 2020) <<https://ssrn.com/abstract=3472887>> accessed 14 June 2021, 10.

forums makes the cautious nature of the initial steps by the Commission understandable. Furthermore, from a fundamental rights perspective, it would have been far worse if the Commission had presented a fixed solution to such an evolving problem as disinformation.⁴⁹

Finally, it appears that the ERGA's overarching recommendation of moving from self-regulation to co-regulation has found sway in the Commission's recent Democracy Action Plan, as will also be discussed in the final section.⁵⁰ Yet before pressing on with the proposed regulatory solutions to disinformation, it is imperative to outline how the Covid-19 pandemic and the associated *Infodemic* brought renewed urgency and attention to the problem of disinformation in the EU.

4. The Covid-19 *Infodemic* – A Novel Challenge

4.1. Background to the *Infodemic*

Like so many problems facing the EU at present, the fight against disinformation can be divided into the period pre-March 2020, and post-March 2020. Although the Covid-19 strain itself proved insidious in wreaking havoc across Europe in a matter of weeks, the virus was also accompanied by a vast web of health disinformation. This associated '*Infodemic*' is defined as 'a flood of information about the virus, often false or inaccurate and spread quickly over social media.'⁵¹ The *Infodemic* is dangerous because of its ability to 'create confusion and distrust and undermine an effective public health response'; it can lead to ignorance of official health advice, wrongful discrimination against minorities, engagement in risky behaviour which prolongs the pandemic, as well as having a detrimental impact on trust in our democratic institutions more generally.⁵²

The spread of Covid-19 disinformation was so menacing because of the interconnectedness between global lockdowns and increased online communications. Social confinement was necessary for public health reasons, yet it limited our social contact and access to information to social media, particularly in March and April 2020. Furthermore, 'given the novelty of the virus, gaps in knowledge proved to be an ideal breeding ground for false or misleading narratives to spread.'⁵³ The manipulation of vulnerable users took many forms, including 'dangerous hoaxes,' 'false health claims,' 'conspiracy theories,' and 'Russian influence operations.'⁵⁴ Moreover, there were issues flowing from disinformation about the origins of the virus which led to 'illegal hate speech' against targeted groups.⁵⁵ Yet as the final section of this article will investigate the feasibility of a *consumer-centric solution* to tackling disinformation, it is necessary to preface this later discussion with an acknowledgement of how the *infodemic* also exposed *consumer protection* issues related to health disinformation.

4.2. The Commission's General Response and the Consumer Protection Issue

The key document which outlines how the impact of Covid-19 disinformation on online consumers in the EU is the Commission's Communication on 'Tackling COVID-19 disinformation' (The June 2020 Communication).⁵⁶ It delineates the different ways in which consumers were exploited during the *Infodemic* through disinformation. Essentially, opportunistic fraudsters and hackers took advantage of consumers' fears and knowledge gaps to cash in on the global crisis, using:

Manipulation, deceptive marketing techniques, fraud, and scams exploit fears in order to sell unnecessary, ineffective and potentially dangerous products under false health claims, or to lure consumers into buying products at exorbitant prices.⁵⁷

⁴⁹ Commissioner for Justice, Consumers and Gender Equality Věra Jourová, statement: 'Should the results under the Code prove unsatisfactory, the Commission may propose further measures, including of a regulatory nature' <https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166> accessed 14 June 2021.

⁵⁰ Commission, Communication on 'the European Democracy Action Plan' (COM/2020/790 final) Section 4.2

⁵¹ Commission, Joint Communication on 'Tackling COVID-19 disinformation - Getting the facts right' JOIN(2020) 8 final, Introduction.

⁵² WHO Report, Coronavirus disease 2019 (COVID-19) Situation Report – 45 (5 March 2020). <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4> accessed 14 June 2021.

It should be noted that the term '*Infodemic*' was originally used in 2003 concerning SARS (*as per* DJ Rothkopf, 'SARS also spurs on Information Epidemic' (Newsday, 14 May 2003).

⁵³ See Commission (June 2020 Communication) (n 51), 1.

⁵⁴ See Commission (June 2020 Communication) (n 51), 1.

⁵⁵ See Commission (June 2020 Communication) (n 51), 1.

⁵⁶ See Commission (June 2020 Communication) (n 51).

⁵⁷ See Commission (June 2020 Communication) (n 51), Section 8.

More concrete examples include the selling of coronavirus ‘miracle products’ with unsubstantiated claims that these products could cure or prevent illness if Covid-19 was contracted.⁵⁸ The June 2020 Communication also highlights how scammers and phishers were using Covid-19 buzzwords such as ‘corona,’ ‘mask’ or ‘vaccine’ to divert traffic to fraudulent websites where users are either tricked into handing over personal data or bank details, or have malware spread into their PC systems; such websites were falsely presented as legitimate state or public health websites.⁵⁹ As discussed in Section I, disinformation has many purposes and although the 2020 Communication does address Russian disinformation campaigns with political motives, the above-mentioned fraud methods were evidently financially motivated. Yet as also discussed in the opening section, the 21st century manifestation of disinformation is so dangerous because of its ability to be unknowingly spread by concerned users without knowledge of the content’s falsity. Thus, user community discussion and debate served to further expand this web of disinformation pushing more users towards scams, as the public struggled to make sense of a virus with so many more questions than answers.

The Commission’s call for an active response to Covid-19 related fraudsters and scammers was largely met by Facebook and Google, *inter alia*, with platforms removing ‘millions of misleading advertisements concerning illegal or unsafe products.’⁶⁰ This was linked with the vast ‘sweep’ of platforms for Covid-19-related fraud and was carried out by the EU’s Consumer Protection Cooperation Network.⁶¹ The ‘sweep’ consisted of two parts: ‘a high-level screening of online platforms, and an in-depth analysis of specific advertisements and websites linked to products in high demand because of the coronavirus.’⁶² For example, Google blocked or removed over 80 million harmful coronavirus-related ads (globally) from March 2020 to May 2020.⁶³

Of course, the value of content moderation statistics released by major platforms is lessened by the lack of transparency as to how many harmful or illegal pieces of content are, in fact, missed by the platforms. Furthermore, an Avaaz report suggests that ‘health misinformation spreading networks generated an estimated 3.8 billion views on Facebook in the last year’ and content from the top ten health misinformation websites had almost four times as many estimated views on Facebook as equivalent content from the websites of ten leading health institutions, including the WHO.⁶⁴

Platforms may nonetheless point to specific measures such as, for example, Facebook banning adverts that ‘imply a product guarantees a cure or prevents people from contracting COVID-19’⁶⁵ and its establishment of the Facebook Coronavirus Information centre.⁶⁶ Thus, despite the Avaaz Report exposing the scale of health disinformation on Facebook, it is clear the platform took a far more interventionist stance in tackling *health disinformation* than previous instances of *political disinformation*. It appears Facebook was more comfortable with being the ‘arbiter of truth’ where coronavirus disinformation existed; it perhaps viewed it as a non-partisan issue where it could simply redirect users to WHO sources, whereas previously the platform had firmly defended its non-interventionist free speech rationale when failing to remove political disinformation.⁶⁷ Interestingly, Facebook deviates from its stance on Covid-19 disinformation where ‘Anti-Vaxxer’ posts are concerned, presumably stemming from the politically charged nature of the Anti-Vaxxer movement.⁶⁸

It is argued that both the Commission and the major platforms correctly acknowledged the unique public health dangers posed by Covid-19 disinformation thus necessitating the prioritisation of an effective public health response over users’ exercising their freedom of expression in sharing mis- or disinformation.

⁵⁸ See Commission (June 2020 Communication) (n 51), Section 8.

⁵⁹ See Commission (June 2020 Communication) (n 51), Section 8.

⁶⁰ Commission, ‘Coronavirus: following Commission’s call, platforms remove millions of misleading ads’ (Press Release, Brussels, 26th May 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_938> accessed 14 June 2021.

⁶¹ See Commission (Press Release) (n 60).

⁶² See Commission (Press Release) (n 60).

⁶³ See Commission (Press Release) (n 60).

⁶⁴ Avaaz, ‘Facebook’s Algorithm: A Major Threat to Public Health’ (Report, Avaaz Disinfo Hub, 19 August 2020) <https://avaazimages.avaaz.org/facebook_threat_health.pdf> accessed 14 June 2021, 2.

⁶⁵ Nick Clegg, ‘Combating COVID-19 Misinformation Across Our Apps’ (Facebook Newsroom, 25 March 2020) <<https://about.fb.com/news/2020/03/combating-covid-19-misinformation/>> accessed 14 June 2021.

⁶⁶ Facebook, Coronavirus Information Centre <https://www.facebook.com/coronavirus_info/> accessed 14 June 2021.

⁶⁷ Tom McCarthy, ‘Zuckerberg says Facebook won’t be ‘arbiters of truth’ after Trump threat’ (The Guardian, 28 May 2020) <<https://www.theguardian.com/technology/2020/may/28/zuckerberg-facebook-police-online-speech-trump>> accessed 14 June 2021.

⁶⁸ Siladitya Ray, ‘Unlike Covid-19 Misinformation, Facebook Won’t Takedown Anti-Vaxxer Posts, Zuckerberg Says’ (Forbes Magazine, 9 September 2020) <<https://www.forbes.com/sites/siladityaray/2020/09/09/unlike-covid-19-misinformation-facebook-wont-takedown-anti-vaxxer-posts-zuckerberg-says/?sh=26ef590c3abb>> accessed 14 June 2021.

Further, unlike in other fundamental rights balancing exercises between freedom of speech and the promotion of informed public debate, here the legal prerequisite exists under EU consumer protection law to remove content where it 'infringes the consumers' acquis and [is thus] illegal content.'⁶⁹

4.3. Lessons learned from the *Infodemic*

To conclude, it is necessary to reflect upon three core findings from the Commission and major platforms' response to the *Infodemic*. Firstly, and as will be discussed in Section IV, the shortcomings of the 2018 Code were exposed during the *Infodemic* by its soft, simplistic nature, with the Commission itself noting its own difficulties in assessing 'the timeliness, completeness and impact of the signatories' actions.'⁷⁰ The 2018 Code's failure to stand up and be counted in the EU's fight against Covid-19 disinformation reinforced the need to 'enforce and strengthen the [Code's] policies.'⁷¹ The second lesson would be that the major platforms' response to the *Infodemic* – although imperfect – demonstrated that these platforms have the tools to clamp down on disinformation when it is seen as a sufficiently serious threat to society.

Finally, the *Infodemic* revealed the various forms of false or misleading content and their respective consequences – and thus, the need to calibrate appropriate responses. For example, disinformation may merely be 'harmful', for instance a Covid-19 conspiracy theory, and thus should be flagged; however, another instance of disinformation may be 'illegal' (under consumer protection law), for instance, a coronavirus 'miracle cure product' scam.⁷² The varying actors in providing disinformation also received renewed attention with the need to calibrate a different response for foreign influence operations motivated to damage EU resilience vis-à-vis opportunistic scammers motivated by the financially lucrative nature of disinformation.⁷³

In reflecting on how best to push forward with the fight against disinformation, two dangerous regulatory consequences must be weighed in the balance:

1. If we under-regulate, disinformation continues to pollute democratic debate and 'alternative truths' become mainstream, and
2. If we over-regulate, mistrust of the state and mainstream media increases. Certain fringe groups may see stricter rules on disinformation as validating the theory that the state is monopolising information. Overly strict laws will inevitably also lead to a chilling effect on free speech in the EU due to self-censorship.

Thus, considering the various regulatory issues exposed by the *Infodemic* – as well as those which predate the crisis – it is submitted that several challenges were presented to the Commission regarding the next concrete steps to tackling disinformation in the EU. It is to these recent steps that we now turn in order to craft out the best path forward in addressing disinformation by analysing the strengths and weaknesses of the EU's Digital Services Act proposal and the importance of presenting long-term solutions to quelling disinformation.

5. Disinformation Regulation in Europe – the Best Path Forward?

5.1. December 2020 – A Call for Stronger Action in Fighting Disinformation

After years of anticipation from European Law academics and tech experts alike, the Commission released its proposal for the Digital Services Act⁷⁴ (from herein referred to as the 'DSA') on 15th December 2020, just two weeks after the European Democracy Action Plan (from herein referred to as the 'DAP'); this Plan largely centred around the dangers of disinformation for European democratic resilience in Europe.⁷⁵ The DAP is particularly informative and serves as a necessary update on why more needs to be done to protect European resilience when faced with large-scale disinformation. In fact, the danger of disinformation pervades all three of the core measures mentioned in the Plan:

⁶⁹ See Commission (June 2020 Communication) (n 51), Section 8.

⁷⁰ See Commission (June 2020 Communication) (n 51), Section 5.

⁷¹ See Commission (June 2020 Communication) (n 51), Section 5.

⁷² See Commission (June 2020 Communication) (n 51), Section 1.

⁷³ It should be noted that this final 'actor' differentiation received considerable attention in the Commission's 2020 Democracy Action Plan (COM[2020] 790 final).

⁷⁴ Commission, Proposal for a Parliament and Council Regulation on Single Market for Digital Services (Digital Services Act) SEC(2020) 432 final.

⁷⁵ Commission, Communication on 'the European Democracy Action Plan' COM(2020) 790 final.

- (1) to promote free and fair elections and strong democratic participation;
- (2) to support free and independent media; and
- (3) to counter disinformation.

Firstly, measure (1) relates to disinformation in that the 2018 Code was established in anticipation of the 2019 European Parliament elections. Ahead of the 2023 elections, political disinformation around election time remains a concern considering its ability to dissuade democratic participation.⁷⁶ Secondly, measure (2) also concerns disinformation in that false and misleading content has eroded trust in trusted, traditional media sources.⁷⁷ Although European Press Councils hold members of the traditional press to professional ethical standards to counteract biases and the publishing of dis- or misinformation, digital-age 'citizen journalists' are free from any such rules; this means that they are not held accountable where blatant biases or disinformation are published online and taken as fact by the user community.⁷⁸ Measure (3) is a direct call to counter disinformation, restating how information is being weaponised by foreign actors and impeding public health efforts in tackling the Covid-19 pandemic; the Commission restates its commitment to imposing stricter content moderation obligations on platforms via the DSA.⁷⁹

Even prior to this, early Commission documents concerning the DSA refer to the emerging 'patchwork of national rules' on content moderation and the need to address this by revising the 'overarching framework for digital services online' in a singular 'Act'.⁸⁰ This 'patchwork' refers to the divergences opening up across the EU in tackling content moderation. For instance, the strict German 'NetzDG'⁸¹ rules have been in place since 2017, yet recent French attempts to follow this approach were struck down by the French Constitutional Court.⁸² The Court held that 'free discourse on social media is not only vital for the maintenance of a democratic society,' but also that an appropriate balance must be struck between 'legislation censoring harmful content and people's right to express their opinions on current affairs.'⁸³ This decision should be commended in that it highlights how the foundational importance of free speech should define the *outer limits* of any future rules on content moderation.

5.2. The Digital Services Act and Disinformation

5.2.1. The Competence Obstacle

Considering the emerging 'patchwork' of national content moderation rules, the DAP's focus on disinformation, and the assessment of the 2018 Code being critical of several issues caused by the self-regulatory approach, it was tempting to expect a vast overhaul of disinformation rules in the DSA.⁸⁴ It appears that this was a step too far for the Commission, outlining in the DAP (and later confirming in the DSA itself) that a 'revised and strengthened Code of Practice on Disinformation' would be drawn up in Spring 2021 as opposed to dealing with disinformation directly within the Regulation.⁸⁵ Although one may be underwhelmed by how disinformation is referred to in the DSA given the continued outsourcing of disinformation moderation to another soft-law 'Code' – albeit a 'strengthened' one – it is necessary to posit three points; two points which somewhat limit this critique at present, and a third point which looks to the possibilities of a primary treaty amendment to correct current shortcomings.

Firstly, the DAP and DSA endorse the move to a 'co-regulatory backstop' model for the measures which would be included in the 2021 Code.⁸⁶ Although this positive step appears to accept the ineffective nature of the self-regulatory model, it remains to be seen if the backstop will provide for 'appropriate enforcement

⁷⁶ See Commission (DAP) (n 75), Section 2.

⁷⁷ See Commission (DAP) (n 75), Section 3.

⁷⁸ Cheryl Iretton, Julie Posetti (eds) 'Journalism, Fake News and Disinformation' (UNESCO Handbook for Journalism Education and Training 2018), 24.

⁷⁹ See Commission (DAP) (n 75), Section 4.

⁸⁰ Commission, 'DGx Proposed Priorities Paper' (2019) <https://www.politico.eu/wp-content/uploads/2019/08/clean_definite2.pdf> accessed 14 June 2021, 24.

⁸¹ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerkdurchsetzungsgesetz] [NetzDG] [Act to Improve Enforcement of the Law in Social Networks], (01/09/2017) BUNDESGESETZBLATT, Teil I [BGBl-I] at 3352.

⁸² Conseil Constitutionnel, 'Loi visant à lutter contre les contenus haineux sur internet' (Décision n°. 2020–801 DC du 18 juin 2020) <<https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm>> accessed 14 June 2021.

⁸³ Conseil Constitutionnel, 'Loi visant à lutter contre les contenus haineux sur internet' (Décision n°. 2020–801 DC du 18 juin 2020) <<https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm>> accessed 14 June 2021.

⁸⁴ See Commission (Code Assessment) (n 39), 21–22.

⁸⁵ See Commission (DAP) (n 75), Section 4.2; see also See Commission (DSA) (n 74), Recital 69.

⁸⁶ See Commission (DSA) (n 74), Recital 68.

mechanisms, sanctions and redress', as recommended by the VVA study in the recent assessment of the 2018 Code.⁸⁷ The DAP statements on this matter are less than inspiring with mere 'calls' for Code signatories to strengthen the Code.⁸⁸

Secondly, and more importantly, the Commission does not have the legislative prerogative to tackle disinformation in a more direct manner; there is no EU competence to craft legislation which attempts to balance online safety with freedom of expression without referring back to the 'internal market' rationale under 114 TFEU, a rationale which, it is argued, is relatively far removed from the specific issue of disinformation (although the rationale can be justified in the DSA more broadly).⁸⁹

Some have argued that this lack of competence has impeded recent digital legislation from respecting free speech as it can only pay 'lip service' to this fundamental right.⁹⁰ This is because although freedom of expression is recognised under Article 11 of the EU Charter of Fundamental Rights, new legislation cannot be adopted on the basis of the Charter. Article 6(1) TEU stresses that '[t]he provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties'⁹¹ and Article 51(2) EUCFR requires that, in interpreting and applying the Charter, the ECJ respects the union principle of conferral.⁹² Thus, at present, it is merely wishful thinking to believe that strictly binding rules on key content moderation issues such as disinformation and hate speech will be dealt with via Article 114 TFEU. The DSA is nonetheless presented by the Commission as 'a horizontal piece of legislation' unintended to 'explicitly address some of the very specific challenges related to disinformation;' it is therefore necessary to await the strengthened 2021 Code for a full critique on the lessons learned from the 2018 Code's failings.⁹³

Yet despite the need to delay critical analysis of the practical effectiveness of the 2021 Code (and its relationship with the DSA), it is nonetheless prudent to briefly examine one mid-term solution in the event of the Code falling short of expectations. Thus, thirdly, one might argue that irrespective of the DSA's positive steps, challenging and pressing issues such as disinformation beg the question of whether the time is ripe for a treaty amendment addressing digital rights and governance in the EU. This amendment could provide an alternative legal basis to Article 114 TFEU's internal market rationale so that the drafting of rules which will have a profound impact on online public discourse (and thus democratic participation more generally) is not primarily seen through the prism of the single market.

Such an amendment may *prima facie* appear unlikely or extreme. However, if the legislative path of general data protection rules over the past 25 years is investigated, it becomes clear that treaty amendments can play a role in correcting the legal basis where fundamental rights are at stake. The GDPR's legislative path was as follows: firstly, the 1995 Data Protection Directive was drawn up using the 'internal market' rationale with reference to the free flow of personal data;⁹⁴ secondly, the 2009 Lisbon Treaty fleshed out data protection significantly in Article 16 TFEU by holding that everyone has the right to the protection of their personal data and allowing the EU legislature to draft new rules relating to this protection.⁹⁵ This was done after it had become apparent that the 1995 Directive and its internal market rationale had led to legislation which *paid insufficient regard for fundamental rights* – in this case, (data) privacy rights; thus, the GDPR was

⁸⁷ See Commission (Code Assessment) (n 39), 22.

⁸⁸ See Commission (DAP) (n 75), Section 4.2.

⁸⁹ See Commission (DSA) (n 74), Section 2 (legal basis): 'In line with this objective, the proposal aims to ensure harmonised conditions for innovative cross-border services... taking into account that several Member States have legislated or intend to legislate on issues such as the removal of illegal content online, diligence, notice and action procedures and transparency.'

⁹⁰ Andrej Savin 'The EU Digital Services Act: What it is and Why it Shouldn't Happen' (EU Internet Law and Policy Blog, 30 July 2019) <<https://euinternetpolicy.wordpress.com/2019/07/30/the-eu-digital-services-act-what-it-is-and-why-it-shouldnt-happen/>> accessed 14 June 2021.

See, for instance: Commission, Proposal for a Regulation on preventing the dissemination of terrorist content online (COM[2018] 640 final); Joris van Hoboken, 'The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications' (Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression, IVIR publications, 3 May 2019).

⁹¹ Treaty on the European Union [2009] OJ C 326/13, Article 6(1).

⁹² EU Charter of Fundamental Rights 2000, Article 51(2); see also: Koen Laenarts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8(3) ECLR 375.

⁹³ Commission, 'Digital Services Act – Questions and Answers (EU-COM website, 15 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> accessed 14 June 2021.

⁹⁴ Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31; preamble.

⁹⁵ Treaty on the Functioning of the European Union [2009] OJ C 326/47, Article 16.

drafted under Article 16 TFEU.⁹⁶ This legislative path should be considered when the Commission assesses its mid-term options in tackling disinformation. Needless to say, such a treaty amendment being approved by member states is no foregone conclusion.

5.2.2. The Substance of the DSA Proposal

Looking to the substance of the DSA itself, some solace can be taken from the Act's suggestion that the 'refusal without proper explanations by an online platform to participate in the application of [Codes] could be taken into account... when determining whether the online platform has infringed the obligations laid down by this Regulation.'⁹⁷ In short, a platform becoming a signatory to, for example, the 2021 Disinformation Code can be considered a risk mitigation measure under Article 27 DSA.⁹⁸ Similarly encouraging is the DSA's 'crisis protocol'; this allows the Commission to draw up a swift, tailored response to address extraordinary circumstances affecting public health or public security such as a future global pandemic.⁹⁹ It is hoped that this protocol will also allow the Commission to also tackle the potential associated *infodemic*. It is also noteworthy that two commitments from the 2018 Disinformation Code became binding in the DSA. Commitment II.B(3) of the Code on enabling public disclosure of adverts find its way into Article 30 DSA obliging the tech giants to compile an ad repository, just as Commitment II.E(12) on data access for researchers appears in Article 31 DSA concerning 'data access and scrutiny.'¹⁰⁰

Further, pragmatic steps to address the unique market power of the world's major platforms is taken in Section 4 of the Act which concerns 'very large online platforms' (platforms with over 45 million active EU users).¹⁰¹ Given the 'systemic risks posed by such platforms, influencing online safety and shaping public opinion', these platforms are subject to additional transparency obligations including 6 monthly assessments for 'any significant systemic risks.'¹⁰² Of particular relevance, considering the 2020 *Infodemic*, is that these 6-month assessments must include reports on the 'intentional manipulation of the service with an actual or foreseeable negative effect' on 'public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.'¹⁰³

Although the above step of differentiating platforms based off the number of active EU users is commendable, the organisation and promotion of the Capitol Hill Riots in Washington on 6th January 2021 also taking place on smaller platforms (such as 'Parlor') demonstrates that this is not a black and white issue of user number.¹⁰⁴ This issue has not (yet) manifested itself in Europe but there is a danger that purveyors of disinformation may relocate to newer platforms subject to less burdensome content moderation rules. This potential 'relocation' could further worsen the problems of online echo chambers and general polarisation in the user community. The Capitol Hill Riots hastened calls within the European Parliament for the DSA to 'double down' on containing the spread of conspiratorial content.¹⁰⁵ Belgian MEP, Kris Peeters, noted the dangers which may lie ahead if more stringent action is not taken at EU level: 'the riots have in large part been fuelled by online conspiracy theories so successful they have completely subverted the trust of many Americans in basic democratic institutions.'¹⁰⁶ One solution to the possibility of content 'relocation' may be to include the aforementioned 'systemic risk' posed by platforms as a categorisation alongside user number so that such problematic platforms can be identified in advance.¹⁰⁷ Yet against this concern of disinformation relocation, one nonetheless needs to acknowledge that this 'very large online platform' differentiation

⁹⁶ Parliament and Council Regulation (EU) 2016/679 of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) [2016] OJ L 119/1, Recital 12.

⁹⁷ See Commission (DSA) (n 74), Recital 68.

⁹⁸ See Commission (DSA) (n 74), See n 74 (DSA) Article 27.

⁹⁹ See Commission (DSA) (n 74), Article 37.

¹⁰⁰ See Commission (DSA) (n 74), Articles 30–31.

¹⁰¹ See Commission (DSA) (n 74), Section 4.

¹⁰² Lorna Woods, 'Overview of Digital Services Act' (EU Law Analysis Blog, Wednesday 16 December 2020) <<http://eulawanalysis.blogspot.com/2020/12/overview-of-digital-services-act.html>> accessed 14 June 2021.

¹⁰³ See Commission (DSA) (n 74), Article 26(1).

¹⁰⁴ Sheera Frankel, 'How the Storming of Capitol Hill Was Organized on Social Media' (New York Times, 6 January 2021) <<https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html>> accessed 14 June 2021.

¹⁰⁵ Samuel Stolton, Philipp Grüll, 'Lawmakers call for tougher EU disinformation laws in wake of US riots' (EURACTIV.com, 8 January 2021) <<https://www.euractiv.com/section/digital/news/lawmakers-call-for-tougher-eu-disinformation-laws-in-wake-of-us-riots/>> accessed 14 June 2021.

¹⁰⁶ Ibid.

¹⁰⁷ See Commission (DSA) (n 74), Article 26(1).

seeks to foster innovation in smaller, up-and-coming platforms by not holding them to costly and onerous content moderation standards.

Finally, it is submitted that those hoping that the DSA would reform EU rules for tackling disinformation will be underwhelmed by the Commission's proposal. Yet given the competence issue discussed above as well as the open possibility that the new co-regulatory backstop will more effectively enforce and sanction platforms falling short of Code commitments, a comprehensive discussion of how the Commission plans to tackle disinformation into the future should be delayed until the 'revised and strengthened' Code is released.

5.3. The Feasibility of a Consumer-Centric Solution?

Lorna Woods, in reflecting upon the DSA proposal, voiced her concerns about potential fundamental rights issues down the line – particularly around 'freedom of expression and the right to private life' given the DSA's indirect encompassing of 'forms of content that are not illegal (disinformation)' via the aforementioned co-regulatory backstop.¹⁰⁸ Furthermore, the freedom of expression issue is likely to be a contentious matter for the EU legislature in the coming months and years as the DSA works itself through the Council and Parliament. Considering the delicate balancing exercise between protecting free speech online versus preventing public debate being based off false or misleading statements, MEPs will here play an indispensable role. Regarding Woods' concerns about 'non-illegal content,' it is again restated that any conclusive findings on the fundamental rights implications of new disinformation rules should be postponed until the release of the 2021 Disinformation Code.

Yet considering all this discussion of finely tuned balancing exercises with considerable fundamental rights implications on either side, it is imperative to look outside the broad, sweeping nature of stricter content moderation by platforms and national authorities. As a matter of practicality, the frequency and commonly disguised nature of disinformation means that it is unrealistic to think that platforms can assess all false or misleading posts – even with hypothetical EU rules directing them how to do so.¹⁰⁹ More importantly, from a fundamental rights perspective, a regulatory approach which fails to appreciate the value of open discourse by prioritising the removal of all misleading posts would undoubtedly infringe EU citizens' freedom of expression and freedom of information rights, under Article 11 of the EU Charter of Fundamental Rights.

Commission statements from the DAP, DSA and the 2018 Code's Assessment do not shy away from the impact which over-regulation would have on free speech online, alongside an acknowledgement of the opposing argument that disinformation may also undermine this fundamental right.¹¹⁰ Indeed, issues around 'the protection of fundamental rights' are noted by the Commission as a limitation 'inherent to the self-regulatory nature of the Code': the importance of upholding these rights is acknowledged in the Code but it 'does not set out procedures to ensure... the protection of these rights in the pursuit of actions addressing disinformation.'¹¹¹ In short, the lack of 'adequate complaint procedures and redress mechanisms' prevents users from accessing a remedy where content is erroneously demoted or deleted.¹¹²

Considering that a more 'heavy-handed' approach to disinformation regulation is fraught with legislative difficulties, it is imperative that academics and legislators alike look elsewhere for long-term solutions to tackling disinformation which are less interventionist and more sustainable. It is submitted that the most important solution in this regard is the *empowerment of the user community* to recognise and report false or misleading content.

The empowerment of consumers is not a novel facet to the Commission's response to disinformation in the EU: the 2018 Code has a specific commitment entitled 'empowering consumers' focused on 'helping people make informed decisions when they encounter online news that may be false.'¹¹³ Similarly, the Commission has more recently held that 'engaged, informed and empowered citizens are the best guarantee

¹⁰⁸ See Woods (n 102).

¹⁰⁹ Davey Alba, 'On Facebook, Misinformation Is More Popular Now Than in 2016' (New York Times, 12 October 2020); there were 1.8 billion interactions on Facebook pages for outlets posting misinformation in the third quarter of 2020, roughly three times the amount in 2016.

¹¹⁰ James Pamment, 'The EU's Role in Fighting Disinformation: Taking Back the Initiative' (Carnegie Endowment, Future Threats, Future Solutions #1, 15 July 2020). <<https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286>> accessed 14 June 2021, 4.

¹¹¹ See Commission (Code Assessment) (n 39), 18–19.

¹¹² See Commission (Code Assessment) (n 39), 19.

¹¹³ See Commission (2018 Code) (n 29), Section II.D.

for the resilience of our democracies.¹¹⁴ In its June 2020 Communication, the Commission further highlighted the importance of 'empowering and raising citizen awareness' as one of the lessons learned from the *Infodemic*.¹¹⁵ Yet it is argued that this response does not sufficiently appreciate why this softer approach is *the core lesson* to be learned from the *Infodemic*.

As presented in Section III, the position of the 'consumer' (or 'user') on platforms is currently multi-faceted and largely context dependent. It is evident that the vulnerability of consumers to coronavirus-related scams in the initial months of the *Infodemic* demonstrated the necessity of EU consumer protection law and the 'sweep' of platforms, removing 'millions of misleading advertisements concerning illegal or unsafe products.'¹¹⁶ Yet it is essential that the EU's future digital strategy *does not solely see online consumers as needing protecting*. Empowering users to recognise false or misleading content is the most sustainable solution to tackling disinformation.

It is submitted that an EU-wide digital media literacy programme should be the foundation upon which the empowerment of the user community can take place into the future.¹¹⁷ At national level, civil society organisations such as 'Article 19' are placing media literacy tools and fact-checking initiatives at the heart of their solutions to disinformation; this is highlighted within their disinformation awareness campaign in Ireland, 'Keep It Real.'¹¹⁸ Although the *Infodemic* demonstrated that victims of disinformation spanned several age groups, it is nonetheless recommended as a long-term strategy to begin media literacy training from the age of 12 up until – and potentially including – third-level education.¹¹⁹ Although research has shown that older persons are more likely to 'share' misinformation, the impressionability of young teens makes them perfect targets for viral disinformation where they do not yet have the critical analysis skills to detect disinformation.¹²⁰ It also appears that young people are aware of their vulnerability to biases, with 40% of them considering that critical thinking, media and democracy are 'not taught sufficiently in school.'¹²¹ The benefits to media literacy skills are apparent and have been succinctly stated elsewhere:

Media literacy skills help citizens check information before sharing it, understand who is behind it, why it was distributed to them and whether it is credible. Digital literacy enables people to participate in the online environment wisely, safely and ethically.¹²²

If EU citizens are given the tools to detect disinformation and political biases, they can form positive online habits; this might include seeking out multiple, verifiable news sources on a contentious story. The knock-on benefits for democratic resilience across Europe are powerful; countering disinformation through education and the promotion of open political debate is 'crucial for effective participation in society and democratic processes.'¹²³

The final benefit of empowering users by investing in digital media literacy education would be that informed users could fill in gaps in the detection of harmful and illegal content. Although 89% of the hate speech detected on Facebook¹²⁴ is done via AI tools, human content moderation still plays a crucial role. Thus, future EU action tackling disinformation should realise the potential of a media-literate user community to detect and report nuanced or disguised instances of harmful or illegal content which AI tools currently fail to detect.

¹¹⁴ See Commission (DAP) (n 75), Section 1.

¹¹⁵ See Commission (June 2020 Communication) (n 51), Section 7.

¹¹⁶ See Commission (June 2020 Communication) (n 51), Section 8.

¹¹⁷ It should be noted that the revised 'Audiovisual Media Services Directive' (2018/1808) already requires Member States to promote the development of media literacy skills and obliges video-sharing platforms to set up effective media literacy tools.

¹¹⁸ Article 19 Organisation, 'Keep it Real – A Campaign on Disinformation and Freedom of Expression in Ireland' (2020–2021) <<https://www.article19.org/campaigns/keep-it-real/>> accessed 14 June 2021.

¹¹⁹ Marianna Spring, 'The casualties of this year's viral conspiracy theories' (BBC News, 26 December 2020) <<https://www.bbc.com/news/blogs-trending-55355911>> accessed 14 June 2021.

¹²⁰ Alex Hern, 'Older people more likely to share fake news on Facebook, study finds' (The Guardian, 10 January 2019) <<https://www.theguardian.com/technology/2019/jan/10/older-people-more-likely-to-share-fake-news-on-facebook>> accessed 14 June 2021.

¹²¹ See Commission (DAP) (n 75), Section 4.2.

¹²² See Commission (DAP) (n 75), Section 4.2.

¹²³ See Commission (DAP) (n 75), Section 4.2.

¹²⁴ Ryan Dansby, Han Fang, 'AI advances to better detect hate speech' (Facebook AI blogpost, 12 May 2020) <<https://ai.facebook.com/blog/ai-advances-to-better-detect-hate-speech/>> accessed 14 June 2021.

Many of these steps are already in motion as part of the Commission's 'Digital Education Plan,' including plans to develop 'common guidelines for teachers and educational staff to foster digital literacy and tackle disinformation through education and training.'¹²⁵ It nonetheless remains to be seen how effectively this Plan will operate in practice and whether it will be in any way interconnected with the upcoming 'strengthened' 2021 Disinformation Code.

Of course, there is an underlying caveat to the finding that the empowerment of consumers is the central solution to curbing the spread of disinformation in the EU: digital media literacy programmes are an impractical solution for the short- and medium term. It is idealistic to think that the user community at present is sufficiently equipped to play a significant role in detecting and reporting disinformation given the politically divisive time that is 2020. As things stand, underlying biases are part of the fabric of the user community; opening the door to user-centric content moderation at present could lead to an even greater 'Fox/ CNN-esque' partisan divide, with different bubbles of the internet propagating their own truth.

It follows that the central limitation to the consumer empowerment solution is the need to accept its inadequacy as a short-term solution. Thus, a stricter co-regulatory framework is needed to address disinformation at the EU level. Despite the aforementioned inherent weaknesses of the continuation of a soft law, voluntary 'Code,' the movement towards a co-regulatory backstop interlinked with the DSA is a step in the right direction. Although the DSA itself does not draw on the importance of user empowerment to tackle disinformation, it is hoped that the upcoming Code will offer more clarity on how platforms, member states and civil society can embrace the value of a well-informed, critical thinking user community in the fight against disinformation.

6. Conclusion

When looking back at the tumultuous year that was 2020, the role of disinformation and its adverse impact on both the Covid-19 public health response and citizens' dwindling trust in democratic institutions will inevitably be a talking point. Although one might argue that *political* disinformation was only an issue for the United States and never truly permeated all Western democracies, it is submitted that the Commission's heightened rhetoric on tackling disinformation indicates an awareness that the next EU disinformation crisis may well be just around the corner. This article has sought to evaluate the Commission's response, beginning firstly with Section I which framed the issue of disinformation in the EU. After exploring the various purposes of disinformation, a discussion of the Commission's response prior to the pandemic was submitted, drawing particularly on the shortcomings of the '2018 Code' (Section II).

Section III described how the Covid-19 *Infodemic* brought renewed attention to the urgency for updated EU rules on disinformation, looking in-depth at the vulnerability of online consumers to scams and frauds using Covid-19 disinformation. Here it was accepted that the EU's 'sweep' of platforms and the platforms proactivity in tackling health disinformation were commendable.¹²⁶ This more interventionist approach to health disinformation demonstrated that major platforms have the tools to effectively address disinformation, and it has now opened the door to greater accountability across all forms of disinformation into the future.¹²⁷ As Paul Barrett has argued, social media companies' response to the pandemic underscores that it's time for them to drop their 'never an arbiter-of-the-truth' line.¹²⁸ Section IV dealt with the Commission's recent DSA proposal and its plans to introduce a 'revised and strengthened' 2021 Disinformation Code. Here it was observed that the intrigue around how disinformation would be dealt with in the DSA did not live up to expectations, yet it was argued that inherent constitutional barriers prevented disinformation from being directly addressed in an EU regulation.

Finally, as the 2021 Code has not yet been released and considering the aforementioned difficulties in ensuring a comprehensive EU-wide regulatory approach, the feasibility of a more 'consumer-centric' solution to disinformation was posited. This solution seeks to empower consumers to detect and report disinformation by providing mandatory EU-wide digital media literacy programmes. This approach would enable the user community to critically analyse content before accepting its validity; improvements in media literacy and critical analysis skills would go some way in ensuring better-informed online public discourse can

¹²⁵ Commission, Communication on the 'Digital Education Plan 2021–2027' COM(2020) 624 final.

¹²⁶ See Commission (June 2020 Communication) (n 51), Section 8.

¹²⁷ Paul M Barrett, 'Social Media Can Be an "Arbiter of the Truth" After All' (Politico, 14 April 2020) <<https://www.politico.com/news/agenda/2020/04/14/social-media-coronavirus-184438>> accessed 14 June 2021.

¹²⁸ Ibid.

take into the future. Of course, 'future' is the key word where this solution is concerned, and its inability to tackle the rampant spread of disinformation in the short- and medium-term is accepted given the frequency of content online and underlying biases built into the user community at present. On this note, it was argued that major shortcomings in the short- or medium-term may necessitate a treaty amendment addressing digital governance such that new rules are not purely drafted using the internal market rationale.

To conclude, a comprehensive regulatory approach to disinformation is necessary. It is imperative that in crafting this approach, the importance of free speech online to promote public debate is weighed up against the importance of regulating disinformation so these same debates are not based on false or misleading information. Consumer empowerment is not the 'be-all-and-end-all' solution to this balancing exercise and the Commission's steps towards a co-regulatory framework are to be commended. Yet consumer empowerment is nonetheless submitted as an *indispensable facet of all other legal solutions* open to the Commission in ensuring a more sustainable, stable online environment into the EU's future. If a mandatory EU-wide digital media literacy programme could be put in place, its potential effect on users would go some way in curbing the scale of disinformation in the next *infodemic* as it inevitably arises.

Competing Interests

Ruairí Harrison completed this article whilst still working as a junior research assistant at the Utrecht School of Law. It should be noted that in March 2021, Ruairí began a traineeship at the European Commission's DG-CONNECT where he now works on the Digital Services Act as part of the F.2 Unit.

Author Information

Considering the contemporary, ever-evolving nature of this topic, it should be noted that this article was last updated substantively on the 15th of February 2021.

How to cite this article: Ruairí Harrison, 'Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 *Infodemic* and the Feasibility of a Consumer-centric Solution' (2021) 17(3) Utrecht Law Review pp. 18–33. DOI: <https://doi.org/10.36633/ulr.675>

Published: 12 October 2021

Copyright: © 2021 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See <http://creativecommons.org/licenses/by/4.0/>.



Utrecht Law Review is a peer-reviewed open access journal published by Utrecht University School of Law.

OPEN ACCESS The Open Access icon, a stylized 'O' with a person inside.