UC Irvine Journal of International, Transnational, and Comparative Law

Volume 6 *Symposium: The Transnational Legal Ordering of Privacy and Speech* Article 3

5-27-2021

Regulating Disinformation in Europe: Implications for Speech and Privacy

Joris van Hoboken
Vrije Universiteit Brussel

Ronan Ó Fathaigh
University of Amsterdam

Regulating Disinformation in Europe: Implications for Speech and Privacy

Joris van Hoboken* & Ronan Ó Fathaigh**

This Article examines the ongoing dynamics in the regulation of disinformation in Europe, focusing on the intersection between the right to freedom of expression and the right to privacy. Importantly, there has been a recent wave of regulatory measures and other forms of pressure on online platforms to tackle disinformation in Europe. These measures play out in different ways at the intersection of the right to freedom of expression and the right to privacy. Crucially, as governments, journalists, and researchers seek greater transparency and access to information from online platforms to evaluate their impact on the health of their democracies, these measures raise acute issues related to user privacy. Indeed, platforms that once refused to cooperate with governments in identifying users allegedly responsible for disseminating illegal or harmful content are now expanding cooperation. However, while platforms are increasingly facilitating government access to user data, platforms are also invoking data protection law concerns as a shield in response to recent efforts at increased platform transparency. At the same time, data protection law provides for one of the main systemic regulatory safeguards in Europe. It protects user autonomy concerning data-driven campaigns, requiring transparency for internet audiences about targeting and data subject rights in relation to audience platforms, such as social media companies.

* Prof. Dr. Joris van Hoboken, Professor of Law, Chair "Fundamental Rights and Digital Transformation," Vrije Universiteit Brussel (VUB), and Associate Professor, Institute for Information Law, Faculty of Law, University of Amsterdam (the Chair at VUB is established at the Interdisciplinary Research Group on Law Science Technology & Society, with the support of Microsoft).
** Dr. Ronan Ó Fathaigh, Senior Researcher, Institute for Information Law, Faculty of Law, University of Amsterdam. The authors would like to thank the participants of the 2020 Symposium on Transnational Legal Ordering of Privacy and Speech (hosted by the UC Irvine School of Law), and the participants of the 2020 Digital Legal Talks conference (hosted by the University of Amsterdam, Tilburg University, Radboud University Nijmegen and Maastricht University) for very helpful comments on earlier drafts of this Article.

INTRODUCTION

There has been a troubling wave of regulation sweeping across Europe targeting disinformation on online platforms, with regulation further accelerating during the Covid-19 pandemic.[1] This regulation has not only taken the form of legislation but has also encompassed other forms of government pressure on platforms to combat disinformation. Indeed, platforms that once refused to cooperate with European governments in identifying users responsible for disseminating allegedly illegal or harmful content are now expanding cooperation.[2] While these developments have profound implications for the right to freedom of expression, there are also complicated implications for the rights to privacy and protection of personal data. This is because greater transparency and access to platform data are considered crucial tools in understanding disinformation and the impact of social media on societies more generally.[3] However, access to data raises acute issues for user privacy, and indeed, platforms are invoking data protection law concerns in response to recent efforts at increased transparency. Such concerns notwithstanding, data protection law provides for one of the main systemic

1. *See* Council of Europe, Comm'r for Human Rights, Press Freedom Must Not Be Undermined By Measures to Counter Disinformation About COVID-19 (2020), https://www.coe.int/en/web/commissioner/-/press-freedom-must-not-be-undermined-by-measures-to-counterdisinformation-about-covid-19 (criticizing measures taken in a number of European countries targeting disinformation during the COVID-19 pandemic); *see also* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Disease Pandemics and the Freedom of Opinion and Expression*, U.N. Doc. A/HRC/44/49 (Apr. 23, 2020).

2. *See* Mathieu Rosemain, *In a World First, Facebook to Give Data on Hate Speech Suspects to French Courts*, REUTERS (June 25, 2019), https://www.reuters.com/article/us-france-tech-exclusive/exclusive-in-a-world-first-facebook-to-give-data-on-hate-speech-suspects-to-french-courts-idUSKCN1TQ1TJ; *see also* Natasha Lomas, *Germany Tightens Online Hate Speech Rules to Make Platforms Send Reports Straight to the Feds*, TECHCRUNCH (June 19, 2020), https://techcrunch.com/2020/06/19/germany-tightens-online-hate-speech-rules-to-make-platforms-send-reports-straight-to-the-feds.

3. *See* Rep. of the Indep. High Level Grp. on Fake News and Online Disinformation, A Multi-Dimensional Approach to Disinformation, at 22 (Mar. 2018) (arguing that "access to platforms' data is key to a better understanding the dissemination patterns of digital disinformation").

regulatory safeguards in Europe against data-driven manipulation, protecting user autonomy in relation to data-driven campaigns, requiring transparency toward users about targeting, and granting data subject rights in relation to online platforms.[4]

The purpose of this Article is to examine the implications of disinformation regulation in the European Union on both the right to freedom of expression and the right to privacy. In particular, the Article addresses the double-edged role operated by European fundamental rights law. On the one hand, government regulation of disinformation represents a danger to the exercise of freedom of expression.[5] On the other hand, under European freedom of expression principles, the state has a positive obligation to create an enabling environment for freedom of expression, including putting in place appropriate legal frameworks to allow a plurality of voices.[6] Similarly, disinformation regulation represents a danger to the right to privacy and data protection (such as surveillance and monitoring of legal content and online expressive and political activity). And yet, European data privacy laws also offer a systemic safeguard for the protection of privacy and personal data.

This Article also discusses the implications of European disinformation regulation and the consequent regulatory pressure being focused on the responsibilities of dominant online platforms, almost all of which are not headquartered in Europe.[7] In this regard, while there are justified criticisms of European disinformation policy, it must be recognized that this policy is quite centrally about the impact these non-EU platforms have on the functioning of European democracies and the responsiveness of these platforms to national laws and conditions.[8] As such, the Article situates European disinformation regulation within the broader framework of transnational legal ordering, where European disinformation regulation can be viewed as a transnational legal order (TLO), comprised of a "collection of formalized legal norms and associated organizations and actors that authoritatively order the understanding and practice of law across national jurisdictions."[9] As described below, European disinformation regulation

4. For a study on data-subject access rights under EU data protection law, see Jef Ausloos & Pierre Dewitte, *Shattering One-Way Mirrors – Data Subject Access Rights In Practice*, 8(1) INT'L DATA PRIV. L. 4, (KU Leuven Centre For IT & IP Law, CiTiP Working Paper 32/2018, 2018).

5. Such as content-based restrictions on political expression.

6. *See* Centro Europa 7 S.r.l. v. Italy, App. No. 38433/09, 2012-III Eur. Ct. H.R. 339, 386–87.

7. Valentina Pop & Sam Schechner, *Tech Giants to Face EU Legal Push on Content, Competition, Taxes*, WALL St. J. (July 5, 2020), www.wsj.com/articles/tech-giants-to-face-eu-legal-push-on-content-competition-taxes-11593967270.

8. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – On the European Democracy Action Plan*, at 2, COM (2020) 790 final (Mar. 12, 2020).

9. *See* TERENCE C. HALLIDAY & GREGORY SHAFFER, *Transnational Legal Orders*, *in* TRANSNATIONAL LEGAL ORDERS 3, 5 (Terence C. Halliday & Gregory Shaffer eds., 2015); *see also* GREGORY SHAFFER & TERENCE C. HALLIDAY, *With, Within, and Beyond the State: The Promise and Limits of Transnational Legal Ordering*, *in* OXFORD HANDBOOK OF TRANSNATIONAL LAW (Peer Zumbansen

involves norms (a) formalized through hard and soft law, (b) produced by EU member states and in conjunction with EU bodies and networks that transcend EU nation-states, and (c) bodies (such as police) within multiple EU member states. All the while, this TLO seeks to settle norms around disinformation across nation-state boundaries in Europe and indeed beyond Europe.

Part I sets out the various forms that current disinformation regulation takes and how such regulation squares with the right to freedom of expression. Part II discusses the implications for the right to privacy, particularly related to police and government access to data and the sharing of user data. Part III then assesses how data protection law may provide a structural safeguard for protecting against the excesses of data-driven disinformation.

I. EUROPEAN DISINFORMATION LAW AND POLICY

The notion of disinformation is but the latest and more palatable offshoot of the much-maligned notion of fake news.[10] Following the widespread use of the term by then-candidate Donald J. Trump in criticizing U.S. media during his 2016 presidential campaign, the term, unfortunately, migrated to Europe. Rather than reject the use of such a term, some policymakers at the EU and national level not only adopted the term but even began proposing legislation to restrict fake news. For example, in early 2017, a bill was introduced in the Italian parliament proposing to criminalize spreading "false, exaggerated, or biased" news reports online.[11] Then, in the summer of 2017, the European Parliament adopted a resolution calling on the European Commission to analyze the legal framework on fake news and consider the possibility of "legislative intervention" to limit the dissemination and spreading of fake content.[12]

Fortunately, rather than rush to implement fake news legislation, an independent high-level expert group (HLEG) was established by the European

ed. 2021); Gregory Shaffer, *Theorizing Transnational Legal Ordering*, 12 ANN. REV. L. & SOC. SCI. 231 (2016).

10. *See* Tarlach McGonagle, *"Fake News": False Fears or Real Concerns?*, 35 NETH. Q. HUM. RTS. 203, 209 (2017) (arguing "accusations of peddling 'fake news' can stigmatize and undermine critical media and erode public trust and confidence in the Fourth Estate."); JORIS VAN HOBOKEN, NAOMI APPELMAN, RONAN Ó FATHAIGH, PADDY LEERSSEN, TARLACH MCGONAGLE, NICO VAN EIJK, & NATALI HELBERGER, THE LEGAL FRAMEWORK ON THE DISSEMINATION OF DISINFORMATION THROUGH INTERNET SERVICES AND THE REGULATION OF POLITICAL ADVERTISING 24 (2019) (discussing how the term is "strongly associated with political and historical strategies to discredit journalists"); Fernando Nuñez, *Disinformation Legislation and Freedom of Expression*, 10 U.C. IRVINE L. REV. 783, 786 (2020) (arguing the term is "not helpful because it has been routinely used to describe subjectively unfavorable content").

11. David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. OL ITA 1/2018, at p. 1 (Mar. 20, 2018).

12. Resolution on Online Platforms and the Digital Single Market, EUR. PARL. DOC. P8_TA(2017)0272 (2017).

Commission, and it wholly rejected the use of the term "fake news," as it was "inadequate," "misleading," and appropriated by politicians to "undermine independent news media."[13] This echoed a separate independent report drawn up for the Council of Europe, which similarly argued against the use of the term due to it being a "mechanism by which the powerful can clamp down upon, restrict, undermine and circumvent the free press."[14] The Commission's expert-group report focused instead on the dangers of disinformation, which was defined as "false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit."[15] The report stated that while disinformation was not necessarily illegal, it can be "harmful for citizens and society at large."[16] In particular, disinformation can threaten the integrity of European media systems and political processes, and represents a special threat to the integrity of elections.[17]

In the growing literature on disinformation, experts distinguish three perspectives on disinformation that require attention: (1) the content perspective, (2) the actor perspective, and (3) the manner of distribution perspective.[18] First, disinformation can be seen from the perspective of the actual content of communications and publication. Something could be qualified as disinformation because the content is false or misleading in particular ways. The content perspective has been relatively dominant in regulatory discussions and public debate. Second, disinformation can be seen with respect to the actors that are behind particular communicative actions. Something could be qualified as disinformation due to the particular involvement of (and potential deliberate confusion about) specific manipulative actors, such as foreign state actors. Third, something can be qualified as disinformation due to the way in which the information is distributed, "encompass[ing] the variety of techniques viral deception actors may use to enhance and exaggerate the reach, virality and impact of their campaigns."[19] Notably, European scholars have begun attempting to measure the

13. Rep. of the Indep. High Level Grp. on Fake News and Online Disinformation, *supra* note 3, at 10.

14. CLAIRE WARDLE & HOSSEIN DERAKHSHAN, COUNCIL OF EUROPE, INFORMATION DISORDER: TOWARD AN INTERDISCIPLINARY FRAMEWORK FOR RESEARCH AND POLICY MAKING 16 (2017).

15. Rep. of the Indep. High Level Grp. on Fake News and Online Disinformation, *supra* note 3, at 13.

16. *Id.* at 35.

17. *Id.* at 12.

18. *See* Camille François, Actors, Behaviors, Content: A Disinformation ABC Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses 2 (Sept. 20, 2019) (Transatlantic High-Level Working Grp. on Content Moderation Online & Freedom of Expression, Working Paper).

19. *Id.* at 4.

actual effects on political attitudes of certain forms and techniques of disseminating manipulated content, such as manipulated political videos known as "deepfakes."[20]

Notably, the report of the high-level expert group created by the Commission focused on the role of online platforms and how they facilitate the production and circulation of disinformation in new ways and on vast scales. The report singled out the data-driven services and mechanisms offered by platforms that are said to be harnessed by those engaging in disinformation, namely: "behavioral data collection, analytics, advertising exchanges, tools for cluster detection and tracking social media sentiment, and various forms of AI/machine learning."[21] Crucially, the report recommended against "[a]ny form of censorship either public or private,"[22] but delivered a range of recommendations to tackle disinformation based on five pillars: (1) enhance the transparency of the digital information ecosystem, (2) promote the use of media and information literacy to counter disinformation, (3) develop tools for empowering users and journalists and foster a positive engagement with fast-evolving information technologies, (4) safeguard the diversity and sustainability of the European news media ecosystem, and (5) conduct continuous research on the impact of disinformation in Europe.[23]

Following the report, the European Commission adopted an influential Communication in 2018, entitled *Tackling online disinformation: a European approach*, which omitted the use of the term fake news and instead focused on disinformation.[24] The Commission defined 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."[25] The Commission did not provide a reference for this definition, but as we and others have noted, it bears a striking resemblance to a number of so-called false news laws that have been found by national supreme courts to violate freedom of expression standards.[26] Significantly, the Commission decided against any form of legislative proposal on disinformation, and instead it took the following approach.

In October 2018, the Commission unveiled the EU Code of Practice on Disinformation, which had been agreed to by several online platforms (Facebook, Google, Twitter, Mozilla, and more recently, Microsoft and TikTok) and advertising

---

20. *See* Tom Dobber, Nadia Metoui, Damian Trilling, Natali Helberger & Claes de Vreese, *Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?*, INT'L J. PRESS/POL. 1 (2020), https://doi.org/10.1177/1940161220944364.

21. *Commission's High Level Expert Group's Report on Fake News and Online Disinformation*, at 22 (Mar. 12, 2018), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271.

22. *Id.* at 5.

23. *Id.* at 5–6.

24. *Commission Communication on Tackling Online Disinformation: A European Approach*, COM(2018) 236 final (Mar. 12, 2018).

25. *Id.* at 3–4.

26. VAN HOBOKEN ET. AL, *supra* note 10, at 41 (giving examples from the Supreme Court of Canada, Supreme Court, of Zimbabwe and Supreme Court of Uganda).

industry associations.[27] The Code was designed to commit online platforms and the advertising industry to a number of objectives set out in five pillars: (1) improve the scrutiny of advertisement placements, in order to reduce revenues of the purveyors of disinformation; (2) increase the transparency of political advertising and issue-based advertising; (3) ensure the integrity of services with regard to accounts whose purpose and intent is to spread disinformation; (4) empower consumers by diluting the visibility of disinformation, improving findability of trustworthy content, and provide users with easily-accessible tools to report disinformation; and (5) empower the research community by providing access to (a) privacy-compliant data for fact-checking and research activities, (b) relevant data on the functioning of their services, and (c) general information on algorithms.[28]

In the process leading to the presentation of the Code, a Sounding Board—established by the European Commission to assess the Code—gave a damning opinion. The Sounding Board stated in no uncertain terms that the "so-called" code of practice was not a code of practice and "by no means self-regulation," as it had "no clear and meaningful commitments, no measurable objectives or [key performance indicators]," and thus, "no possibility to monitor process, and no compliance or enforcement tool."[29]

In December 2020, the newly appointed European Commission published its proposed reforms of the EU legislative framework applying to online platforms, known as the Digital Services Act (DSA).[30] The proposed DSA imposes a range of new obligations on certain large platforms, including transparency obligations relating to content moderation systems,[31] recommender systems,[32] online advertising,[33] and independent audits.[34] Crucially, certain large platforms will be required to manage "systemic risks" stemming from the functioning and use of their service in the EU, such as the dissemination of illegal content and "intentional manipulation of their service."[35] These systematic risks may also take the form of "coordinated operations aimed at amplifying information, including disinformation, such as the use of bots or fake accounts for the creation of fake or misleading

27. Preamble, EU CODE OF PRACTICE ON DISINFORMATION (2018), https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation [hereinafter EU CODE OF PRACTICE].

28. *Id.* § IIA–IIB.

29. Sounding Bd. of the Multi-Stakeholder Forum on the Code of Practice, *The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice* (Sept. 24, 2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54456.

30. *See Regulation of the European Parliament an of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*, COM (2020) 825 final (Dec. 15, 2020).

31. *Id.* at 50.

32. *Id.* at 61.

33. *Id.* at 31.

34. *Id.* at 61.

35. *Id.* at 59–60.

information."[36] Further, in order to "facilitate supervision and research" in relation to disinformation,[37] certain large platforms will be required to make publicly available repositories of online advertising displayed on their platforms.[38]

A. Transparency and Access to Platform Data

A major European policy objective for tackling disinformation, and indeed other problems associated with platforms, is greater transparency of platform ecosystems and access to platform data.[39] These have been advocated by expert groups, academia, civil society, journalists, and regulators. For example, the High-Level Expert Group on disinformation emphasized that access to platform data was "key to a [sic] better understanding the dissemination patterns of digital disinformation,"[40] to understanding scale and scope of disinformation problems, and, crucially, to allowing proper evaluation of the efficiency of responses.[41] In particular, the Expert Group recommended that platforms should "enable privacy-compliant access to data for the identification of online disinformation actors, for the assessment of fact-checking and debunking strategies and for the study of disinformation dynamics by academics."[42] A prominent role for academic research was also highlighted. The Expert Group recommended that platforms provide data on the "functioning of their services including data for independent investigation by academic researchers and general information on algorithms in order to find a common approach to address the dissemination and amplification of disinformation."[43]

As mentioned above, the EU Code of Practice on Disinformation has a specific pillar dedicated to access to platform data, with platforms committing to "support good faith independent efforts to track disinformation and understand its impact." This commitment includes "sharing privacy protected datasets" and not prohibiting or discouraging good faith research into disinformation and political advertising on their platforms."[44] The European Regulators Group for Audiovisual Media Service (ERGA), which comprises the heads of national audiovisual regulators from each EU member state, was tasked with monitoring the

36. *Id.* at 84.

37. *Id.* at 82–83.

38. *Id.* at 62.

39. For a discussion of current sources of information on platforms' content moderation, see Daphne Keller & Paddy Leerssen, *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation*, *in* SOCIAL MEDIA AND DEMOCRACY: THE STATE OF THE FIELD AND PROSPECTS FOR REFORM 220-51 (Nathaniel Persily & Joshua A. Tucker eds., 2020).

40. Rep. of the Indep. High Level Grp. on Fake News and Online Disinformation, *supra* note 3, at 22.

41. *Id.*

42. *Id.* at 25.

43. *Id.* at 33.

44. EU CODE OF PRACTICE, *supra* note 27, § II.E.

implementation of the Code of Practice.[45] ERGA published a report in June 2020 on the implementation of the Code's data access commitments, which contains considerable criticism of platforms' progress with providing access to data.[46]

The ERGA report stated that there were "enormous difficulties" for researchers to get access to data. Platforms do not share "crucial data points, including data on ad targeting and user engagement with disinformation," and the most important questions about the extent and impact of disinformation "remain unanswered."[47] The report does mention that in 2018, Facebook launched Social Science One as an "ad hoc program aimed at partnering with academics and sharing privacy protected datasets."[48] However, in late 2019, the Co-Chairs and European Advisory Committee of Social Science One published a statement expressing frustration, as "Facebook has still not provided academics with anything approaching adequate data access."[49] The statement strongly articulated that the "current situation is untenable," as "[h]eated public and political discussions are waged over the role and responsibilities of platforms in today's societies, and yet researchers cannot make fully informed contributions to these discussions" and "are mostly left in the dark, lacking appropriate data to assess potential risks and benefits."[50]

ERGA has recommended that platforms be required to share data for research purposes,[51] and indeed, the EU's proposed DSA contains substantive new rules on access to data.[52] An important part of the proposal is the creation of new, dedicated national regulatory bodies (Digital Services Coordinators), which would be empowered to employ large online platforms to access data that are necessary to monitor and assess compliance with the proposed legislation.[53]

---

45. *Commission and High Representative Joint Communication on the Action Plan Against Disinformation*, JOIN (2018) 36 final, 9 (May 12, 2018) ("The Commission will, with the help of the European Regulators Group for Audio-visual Media Services (ERGA) monitor the implementation of the commitments by the signatories of the Code of Practice.").

46. *See* Eur. Reguls. Grp. for Audiovisual Media Servs. (ERGA), *ERGA Rep. on Disinformation: Assessment of the Implementation of the Code of Practice* (2020), https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.

47. *Id.* at 38.

48. *Id.* at 35. *See* SOCIAL SCIENCE ONE, https://socialscience.one (last visited Jan. 17, 2021).

49. *Public Statement From the Co-Chairs and European Advisory Committee of Social Science One,* SOCIAL SCIENCE ONE (Dec. 11, 2019), https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one.

50. *Id.*

51. Eur. Reguls. Grp. for Audiovisual Media Servs. (ERGA), *supra* note 46, at 40.

52. *See Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*, *supra* note 30, at 62–63.

53. *Id.*

B. Content-Based Restrictions on Disinformation

Up to this point in the discussion, the whole premise of EU policy on disinformation has been that disinformation is not *per se* illegal, but it is harmful, and the Commission has always distinguished between illegal content (such as child abuse material) and harmful content (such as disinformation).[54] However, there is a growing realization that disinformation may already be or may become prohibited and criminalized in a number of EU member states, with more seeking to do so during the Covid-19 pandemic.[55] Thus, there is an acute danger of European and national policy-makers focusing on a notion where there already exist very broad and vague laws open to particular abuse.

One of the most notable national laws containing content-based restrictions on disinformation was France's 2018 law on the fight against the manipulation of information.[56] The law provides that during the three months prior to an election, a court can order an online platform to remove "inaccurate or misleading allegations or imputations of fact," which may "alter the sincerity of an upcoming vote" and are "disseminated deliberately, artificially or automatedly," and on a massive scale.[57] The court is required to deliver a decision within forty-eight hours, and any appeal decision must be delivered within forty-eight hours.[58] However, what is rarely discussed is that France has criminalized publication of "false news" under its Freedom of the Press Law 1881 for many years,[59] while Article 97 of the Electoral Code makes it a criminal offence to spread "false news" with the effect of distorting the outcome of an election.[60] Indeed, François Fillon, the former Prime Minister of France who was recently convicted of embezzling public funds,[61] used this false news provision to file a criminal complaint against the newspaper that originally published the allegations against him during the 2017 presidential elections.[62]

---

54. *See Commission Communication on Tackling Online Disinformation: A European Approach*, *supra* note 24.

55. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Tacking COVID-19 Disinformation – Getting the Facts Right*, JOIN (2020) 8 final (June 10, 2020).

56. Loi 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [Law 2018-1202 of December 22, 2018 on the fight against the manipulation of information], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE].

57. *Id.*

58. Loi du 29 juillet 1881 sur la liberté de la presse [Law of 29 July 1881 on freedom of the press], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], art. 27.

59. *Id.*

60. Code électoral [Electoral Code] art. L97.

61. Aurelien Breeden, *François Fillon, Ex-Presidential Hopeful in France, Is Convicted of Embezzlement*, N.Y. TIMES, June 29, 2020, at A10.

62. Saim Saeed, *François Fillon Claims Le Canard Enchainé Illegally Influenced French Election,* POLITICO (May 3, 2017), https://www.politico.eu/article/francois-fillon-claims-le-canard-enchaine-illegally-influenced-french-election.

France is not alone in its content-based restrictions, and similar provisions exist in a number of other EU member states. First, Malta's Criminal Code criminalizes spreading false news, which is defined as "maliciously spreading false news which is likely to alarm public opinion or disturb public good order or the public peace or to create a commotion among the public or among certain classes of the public."[63] Second, Lithuania's Law on the Provision of Information to the Public prohibits the dissemination of disinformation, which is defined as "intentionally disseminated false information."[64] Third, section 264 of Austria's Criminal Code also criminalizes the dissemination of false news during an election or referendum.[65] Fourth, under Article 191 of Greece's Criminal Code, "causing fear" by disseminating false news via the Internet is a criminal offence.[66] Fifth, under Poland's Local Elections Act, a court may issue an order restraining the publication of "untrue data or information" about an election candidate.[67]

There have also been a number of content-based restrictions enacted more recently during the Covid-19 pandemic targeting the notion of disinformation. For example, Romania's 2020 Presidential Decree permitted the communications regulator to order the removal of and block access to online content that "promotes false news" regarding Covid-19 protection and prevention measures.[68] Similarly, Hungary enacted Act XII of 2020 on containment of coronavirus, which amended the Criminal Code's definition of "scaremongering" to include the dissemination of "any untrue fact or any misrepresented true fact with regard to the public danger that is capable of causing disturbance or unrest in a larger group of persons at the

63. CRIMINAL CODE, ART. 82 (amended by the Media and Defamation Act, 2018).

64. Law on the Provision of Information to the Public, No I-1418, art. 2(13) (1996), *amended by* No XII-2239 of Dec. 23 2015.

65. Strafgesetzbuch [StGB] [Penal Code] § 264 [Verbreitung falscher Nachrichten bei einer Wahl oder Volksabstimmung] [Dissemination of false news in an election or referendum] (Austria); *see* Dr. Walter Berka & Dr. Josef Trappel, Internet Freedom in Austria: A Survey Based on the Recommendation CM/Rec(2016)5 of the Committee of Ministers of the Council of Europe to the Member States Regarding Internet Freedom 31 (Jan. 2018) (unpublished manuscript), https://rm.coe.int/report-of-austria-to-the-council-of-europe-following-recommendation-cm/16808c6194 ("[D]istribution of false rumours and manipulated news on the Internet violates existing legislation only in exceptional cases, such as when false news is distributed during an election period or referendum (sec. 264 StGB).").

66. POINIKOS KODIKAS [P.K] [CRIMINAL CODE] 4619:191 (Greece).

67. Ordynacja wyborcza do rad gmin, rad powiatów i sejmików województw [Law of 16 July 1998 on Elections to Municipalities, District Councils and Regional Assemblies] (Dz.U. 1998 Nr 95 poz. 602) § 72.

68. Decret semnat de Preşedintele României, domnul Klaus Iohannis, privind instituirea stării de urgenţă pe teritoriul României, 16 martie 2020 [Decree Signed by the President of Romania, Mr. Klaus Iohannis, Regarding the Establishment of the State of Emergency on the Romanian Territory, Mar. 16, 2020] art. 54, https://www.presidency.ro/ro/media/decret-semnat-de-presedintele-romaniei-domnul-klaus-iohannis-privind-instituirea-starii-de-urgenta-pe-teritoriul-romaniei; *see COVID-19: Restrictions on Access to Information in Romania,* EUR. FED'N JOURNALISTS (Mar. 29, 2020), https://europeanjournalists.org/blog/2020/03/29/covid-19-restrictions-on-access-to-information-in-romania/.

site of public danger" or "any untrue fact or any misrepresented true fact that is capable of hindering or preventing the efficiency of protection."[69] Further, Bulgaria also adopted draft legislation criminalizing the spread of "internet misinformation" and granted the media regulator the power to suspend websites for distributing misinformation.[70] These are all national legislative measures adopted by EU member states that are content-based restrictions applying to the notion of online disinformation.

C. Law Enforcement Involvement

While European policy does not treat disinformation as illegal content, a particular feature of European *practice* on disinformation is the involvement of law enforcement. A concerning example from a freedom of expression perspective can be found in Italy where, in the run-up to the 2018 elections, the Ministry of the Interior implemented an online reporting service known as the Red Button Protocol. Under this Protocol users could "indicate the existence of a network of content attributable to fake news."[71] Notably, the *Polizia Postale*, a police unit that investigates online crime, was responsible for reviewing reports. After reviewing the information, the police could pursue legal action if it determined that the content is unlawful.[72] The UN Special Rapporteur on freedom of expression was particularly critical of this mechanism, expressing concern that under international standards of freedom of expression the restrictions established by the Protocol were "inconsistent with the criteria of legality, necessity and proportionality."[73] In particular, the Protocol could have a particularly strong "chilling effect" on the exercise of the right to freedom of expression as the Protocol could function as a "pipeline" for criminal prosecutions.[74]

Similarly, in the run-up to the 2018 elections in Spain, the Ministry of the Interior announced that teams of police officers would trawl the internet for signs of fake news and "keep a particularly close eye" on social media platforms as part

69. 2020. évi XII (Act XII of 2020 on the containment of coronavirus), at § 10(2), amending the Criminal Code, § 337 ("Scaremongering") (Hung.); *see* Gábor Polyák, "*Enabling Act" in Hungary: Uncontrolled Government Power, Threatened Press*, INTERNET POL'Y REV. (Apr. 9, 2020), https://policyreview.info/articles/news/enabling-act-hungary-uncontrolled-government-power-threatened-press/1466.

70. *See* Press Release, Org. for Sec. & Coop. in Europe (OSCE), COVID-19 Response in Bulgaria Should Not Curb Media Freedom, Says OSCE Representative on Freedom of the Media (Apr. 15, 2020), https://www.osce.org/representative-on-freedom-of-media/450193.

71. Kaye, *supra* note 11, at 1; *see also* Angela Giuffrida, *Italians Asked to Report Fake News to Police in Run-up to Election*, GUARDIAN (Jan. 19, 2018), https://www.theguardian.com/world/2018/jan/19/italians-asked-report-fake-news-police-run-up-election.

72. Kaye, *supra* note 11, at 2.

73. *Id.* at 4.

74. *Id.*

of the election security plan.[75] During the Covid-19 pandemic, free speech organizations such as Article 19 have criticized Spanish police involvement in targeting individuals suspected of spreading disinformation.[76] In February 2020, Spanish prosecutors initiated the first lawsuit for spreading fake news and publicly identified the woman involved.[77] Similarly, in Hungary, the police have arrested individuals on suspicion of spreading fake news.[78] In the Netherlands, law enforcement agencies have posted videos on Facebook warning about the dangers of fake news.[79]

Further, elected officials seek to publicize the involvement of law enforcement where disinformation is concerned. For example, in November 2018, a Member of the European Parliament publicized a complaint submitted to Portuguese police, Belgian police, and Europol regarding a "fake news" website. The Member requested that Europol investigate the website, identify who was behind it, and "demand the removal of all defamatory content."[80] In Spain, members of parliament have also filed a number of criminal complaints against individuals for sharing hoaxes about the government's response to the pandemic. These complaints cite laws criminalizing "calumny" and "insult" to state institutions under the Spanish Penal Code.[81] It is unclear whether fake news and disinformation are criminal offences and, moreover, whether the involvement of law enforcement is an appropriate remedy.

D. Pseudo-Militarization of Disinformation Policy

A further concerning pillar of European disinformation policy that has emerged is the involvement of the foreign policy arms of the EU and its member

75. *Spanish Police to Watch Web for Fake News Before Vote*, REUTERS (Mar. 15, 2019), https://www.reuters.com/article/spain-politics-news/spanish-police-to-watch-web-for-fake-news-before-vote-idUSL8N2123OP.

76. *Spain: Concerns as Penal Code Used to Criminalise Jokes and Misinformation About Coronavirus*, ARTICLE 19 (Apr. 17, 2020), https://www.article19.org/resources/spain-penal-code-used-to-criminalise-jokes-and-misinformation-about-coronavirus/.

77. *Id.*; *see also* AFP, *Spanish Prosecutors File Pioneering Lawsuit Against 'Fake News'*, LOCAL: SPAIN (Feb. 28, 2020), https://www.thelocal.es/20200228/spanish-prosecutors-file-first-lawsuit-against-fake-news.

78. *See* Justin Spike, *He Criticized the Government on Facebook, and Was Taken From His Home by Police at Dawn*, INSIGHTHUNGARY (May 12, 2020), https://insighthungary.444.hu/2020/05/12/he-criticized -the-government-on-facebook-and-was-taken-from-his-home-by-police-at-dawn.

79. *See* Politie Amsterdam, *Voorkom verspreiding van nepnieuws: denk voor je deelt* [*Prevent the Spread of Fake News: Think Before Sharing*], FACEBOOK (Mar. 25, 2020), https://www.facebook.com/watch/?v=214686616405935.

80. Letter from Ana Gomes, Member of the European Parliament, to Catherine De Bolle, Executive Director of Europol (Nov. 20, 2018), https://www.anagomes.eu/PublicDocs/25b1d52c-715a-42da-b3fa-920d499ad5a6.pdf; *see also Rosianne Cutajar Reacts to Criminal Complaint by Gomes Over Online Article*, TIMES MALTA (Nov. 28, 2018).

81. *Spain: Concerns as Penal Code Used to Criminalise Jokes and Misinformation About Coronavirus*, *supra* note 76.

states stimulated by the pseudo-militarization of disinformation policy. Most striking is the language being used in relation to disinformation, which is generally framed around conflict, combat, weapons, and defense. Josep Borrell, the EU's High Representative of the Union for Foreign Affairs and Security Policy, has spoken of how disinformation "can kill," and in today's society, "warriors wield keyboards rather than swords" with disinformation campaigns being a recognized "weapon" that the EU must "fight."[82] This foreign policy aspect of disinformation is built upon a number of efforts based on data and information sharing and the monitoring of the online environment.[83]

First, the EU established the EU Rapid Alert System (RAS) on disinformation. The RAS is a "secure digital platform" and "dedicated technological infrastructure," where EU member states and EU institutions can issue alerts on disinformation and facilitate "sharing of data and assessments."[84] Each EU member state is required to designate a contact point, and platforms must "cooperate with the contact points underpinning the Rapid Alert System, in particular during election periods."[85] There is little transparency about the operation of the RAS. Governments have neither disclosed what content, data, and information are being shared nor how the platforms have responded. But a report published after the 2019 European Parliament elections stated that there had been "daily exchanges and sharing of information," and, indeed, the RAS had "strengthened cooperation with platforms, although the platforms still need to become more responsive to external reports."[86] Notably, the RAS has facilitated cooperation with NATO and will be "further strengthened in the future."[87] Indeed, EU officials have stated how during the Covid-19 pandemic, "we need to continue to work with the platforms, to ask to remove a lot of messages," but "we need to think about a regulation because we don't have for the moment the capacity to go further than that."[88]

Second, disinformation is now considered by the EU to be what is called a hybrid threat, alongside radicalization and violent extremism.[89] For this reason, the EU Hybrid Fusion Cell was established within the EU Intelligence and Situation Centre of the EU's European External Action Service to monitor and address

82. European Commission Press Release IP/20/1006, Coronavirus: EU Strengthens Action to Tackle Disinformation (June 10, 2020).

83. *Action Plan Against Disinformation*, *supra* note 35, at 5–8.

84. *Id.* at 7.

85. *Id.*

86. *Report on the Implementation of the Action Plan Against Disinformation*, at 3, JOIN(2019)12 final (June 14, 2019).

87. *Id.* at 3–4.

88. *See* Samuel Stolton, *Regulation Against Fake News 'Very Important,' Reynders Says*, EURACTIV (Apr. 15, 2020), https://www.euractiv.com/section/digital/news/regulation-against-fake-news-very-important-reynders-says.

89. *Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*, at 3, JOIN(2018)16 final (June 13, 2018).

hybrid threats by foreign actors, including disinformation.[90] Notably, in 2018, expert staff were added to engage in "data mining and analysis to process the relevant data;" to provide "additional media monitoring services to cover a wider range of sources and languages;" and to invest in "analytical tools," such as "dedicated software to mine, organise and aggregate vast amounts of digital data."[91]

Third, the European Council established the East Stratcom Task Force, also within the European External Action Service, to engage in "tracking and tackling disinformation."[92] According to the EU, this monitoring has resulted in over 6,500 individual disinformation cases, many of which deliberately target Europe."[93] This has been done through a service called *EUvsDisinfo* run by the East Stratcom Task Force. By using "data analysis and media monitoring services," *EUvsDisinfo* "identifies, compiles, and exposes disinformation cases."[94] However, *EUvsDisinfo* has faced criticism. Three Dutch news outlets initiated legal proceedings for their inclusion on the disinformation repository after various news articles they had published were publicly classified as disinformation.[95] A few days before the court hearing, the articles were removed from the repository and a correction was included.

E. Implications for Freedom of Expression

The current path being taken by European governments to regulate disinformation has profound implications on freedom of expression. First, under international human rights standards, the four special international mandates on freedom of expression have been quite forthright 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

90. *Commission Communication on Tackling Online Disinformation: A European Approach*, *supra* note 24, at 16.

91. *Commission and High Representative Joint Communication on the Action Plan against Disinformation*, *supra* note 45, at 5.

92. *Id.* at 2.

93. *Id.*

94. *See EUvsDisinfo: Disinformation Operations About COVID-19*, EU OPEN DATA PORTAL (Apr. 6, 2020), https://data.europa.eu/euodp/en/data/dataset/euvsdisinfo-disinformation-operations-about-covid-19.

95. *See* Michael Peel, Mehreen Khan, & Max Seddon, *EU Attack on Pro-Kremlin 'Fake News' Takes a Hit*, FIN. TIMES (Apr. 2, 2018), https://www.ft.com/content/5ec2a204-3406-11e8-ae84-494103e73f7f; Cent. Eur. News, *Three Dutch Media Outlets to Take the EU to Court in 'Misinformation' Spat*, PRESS GAZETTE (Feb. 21, 2018), https://www.pressgazette.co.uk/three-dutch-media-outlets-to-take-the-eu-court-in-misinformation-spat/; Emiel Jurjens & Jens van den Brink, *Recent Experience Shows EU Measures Against Fake News Are Problematic*, MEDIA REP. (May 15, 2018), http://www.mediareport.nl/en/press-law/15052018/recent-experience-shows-eu-measures-against-fake-news-are-problematic/.

standards for restrictions on freedom of expression," and "should be abolished."[96] Similarly, the UN Special Rapporteur on freedom of expression has stated that disinformation is an "extraordinarily elusive concept to define in law" and is "susceptible to providing executive authorities with excessive discretion to determine what is disinformation, what is a mistake, what is truth."[97] As such, the "penalization of disinformation is disproportionate" and results in "deterring individuals from sharing what could be valuable information."[98] Unfortunately, some EU member states, as described above, are enacting and have existing laws on disinformation, false information, and false news, which are difficult to reconcile with international freedom of expression standards.

With respect to the proper legal standard for regulation of disinformation in Europe, the European Court of Human Rights (ECtHR) has delivered a number of judgments on false information legislation that are instructive. The Court has delivered three unanimous judgments concerning a provision under Polish election legislation, which allows election candidates to apply to a regional court for an order restraining publication of campaign material or statements containing "untrue data or information," with the court required to examine the application "within 24 hours."[99] Notably, the ECtHR has found in all three judgments, including in a 2019 judgment, that various proceedings under this provision violated Article 10 of the European Convention on Human Rights (ECHR).[100] For instance, in *Brzeziński v. Poland*, the Court unanimously found a violation of Article 10 because domestic courts had "immediately classified as lies" statements made by a local politician during an election, and "[b]y following such an approach the domestic courts effectively deprived [the politician] of the protection afforded by Article 10."[101] Further, in *Kwiecień v. Poland*, the Court found serious deficiencies under proceedings for "untrue information" during an election and even held that the "fairness of the proceedings may be called into question."[102] Similarly, in *Kita v. Poland*, the Court unanimously found a violation of Article 10 over "untrue information" proceedings, holding that the courts "unreservedly qualified all of [the statements] as statements which lacked any factual basis," and the "standards applied" by the courts were "not compatible with the principles embodied in Article 10."[103] In general, these cases

96. Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, FOM.GAL/3/17, (Mar. 3, 2017), https://www.osce.org/files/f/documents/6/8/302796.pdf.

97. Kaye, *supra* note 1, at 13.

98. *Id.*

99. *See* Brzeziński v. Poland, App. No. 47542/07 at 7 (2019), http://hudoc.echr.coe.int/eng?i=001-194958.

100. *See id.*; Kwiecień v. Poland, App. No. 51744/99 (2007), http://hudoc.echr.coe.int/eng?i=001-78876; Kita v. Poland, App. No. 57659/00 (2008), http://hudoc.echr.coe.int/eng?i=001-87424.

101. Brzeziński, App. No. 47542/07 at 13.

102. Kwiecień, App. No. 57659/00 at 18.

103. Kita, App. No. 57659/00 at 11.

demonstrate that there are serious questions about the compatibility of legislation that seeks to target false information, but does not allow for examination of whether there has actually been undue harm to reputation or candidates' personality rights.

The government-platform initiatives also warrant close scrutiny. The human rights group Article 19 has expressed its concern over EU disinformation policy as it is "plac[ing] increasing pressure on tech companies to monitor and remove content on their platforms," and during the pandemic, platforms "rely more on automated content takedowns, with a reduced and remote workforce."[104] We must remember that this is all happening outside of a clear legal framework and may involve information that is perfectly legal, but considered objectionable by EU and national governmental officials. Damian Tambini has argued how vague and subjective the notion of disinformation is, which can include content that is legal, but "subjectively undesirable."[105] Thus, public officials have great latitude in the type of content that may be labelled disinformation and may end up targeting expression (however objectionable) that clearly constitutes expression on matters of public interest. These types of government-platform initiatives, which operate outside a legislative footing, raise acute issues for freedom of expression and accountability. Similar systems involving government-platform cooperation are the EU's code of practice on hate speech, the EU Internet Forum, the EU Crisis Protocol, and the Global Internet Forum to Counter Terrorism (GIFCT), which has been criticized by a range of NGOs due to the "risks involved in content removal coordination among companies."[106]

II. IMPLICATIONS FOR PRIVACY AND DATA PROTECTION

The regulation of disinformation also has distinct implications for the right to privacy and protection of personal data. This is because disinformation regulation and policy are resulting in increased monitoring and surveillance of the online environment and increased access to user data from platforms. As the UN High Commissioner for Human Rights has stated, government monitoring of information that is publicly available about a person, such as social media posts, undoubtedly implicates the right to privacy.[107]

---

104. *EU Communication on Tackling Coronavirus Disinformation,* ARTICLE 19 (June 11, 2020), https://www.article19.org/resources/europe-eu-communication-on-tackling-coronavirus-disinformation/.

105. *See* DAMIAN TAMBINI, MEDIA FREEDOM, REGULATION AND TRUST: A SYSTEMIC APPROACH TO INFORMATION DISORDER 21 (2020), https://rm.coe.int/cyprus-2020-new-media/16809a524f.

106. Access Now, et al., *Joint Letter to New Executive Director, Global Internet Forum to Counter Terrorism*, Hum. Rts. Watch (July 30, 2020, 1:00 PM), https://www.hrw.org/news/2020/07/30/joint-letter-new-executive-director-global-internet-forum-counter-terrorism.

107. U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/39/29, ¶ 6 (Aug. 3, 2018).

A. Online Monitoring and Disinformation

As described above, there is a whole array of EU and national agencies now engaged in monitoring the online environment in some form. Police forces in various EU member states are engaged in monitoring online discussions in order to identify disinformation and make arrests.[108] Both Europol and Interpol have detailed reports on the activities of national law enforcement in monitoring the online environment for disinformation.[109] Although transparency is generally considered positive, it may be problematic when law enforcement agencies constantly remind individuals that they are monitoring and surveilling the online environment. In Hungary, police officers arrested individuals who posted online comments on the government's response to Covid-19. The police officers filmed and posted search-and-seizure and arrest videos to the national police force's YouTube channel.[110] The police also released statements reiterating that its cybercrime unit "continuously monitors the content related to the infection on the Internet."[111]

A report on online disinformation written for the French Ministry for Europe and Foreign Affairs and Ministry for the Armed Forces included a recommendation of increased surveillance of "risk communities," such as "extremist, conspiratorial and religious groups," in order to "better grasp the communities that propagate false information on the social networks."[112] Once accounts are identified, authorities should engage in "naming and shaming" by naming the source and "discredit[ing] the content of the fake news story—either directly, in an official manner, or indirectly."[113]

---

108. For the situation outside of the EU, see Mu Sochua, *Coronavirus 'Fake News' Arrests Are Quieting Critics*, FOREIGN POL'Y (May 22, 2020, 9:23 AM), https://foreigsnpolicy.com/2020/05/22/coronavirus-fake-news-arrests-quiet-critics-southeast-asia/.

109. *See Interpol Report Shows Alarming Rate of Cyberattacks During COVID-19,* INTERPOL (Aug. 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19; EUROPOL, CATCHING THE VIRUS: CYBERCRIME, DISINFORMATION AND THE COVID-19 PANDEMIC (2020), https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic.

110. Alasdair Sandford, *Hungary: 'Critics Silenced' in Social Media Arrests as EU Debates Orban's Powers*, EURONEWS (May 15, 2020), https://www.euronews.com/2020/05/14/hungary-critics-silenced-in-social-media-arrests-as-eu-debates-orban-s-powers; Andras Gergely & Veronika Gulyas, *Orban Uses Crisis Powers for Detentions Under 'Fake News' Law*, BLOOMBERG (May 13, 2020), https://www.bloomberg.com/news/articles/2020-05-13/orban-uses-crisis-powers-for-detentions-under-fake-news-law; ORFK Communication Service, *Not Only Did He "Produce," He Also Spread The Horror News* (Mar. 15, 2020, 13:55), http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/nemcsak-gyartotta-terjesztette-is-a-remhirt (video uploaded by the Hungarian National Police Communication Service, showing arrest of suspect for spreading false rumors).

111. *Id.*

112. JEAN-BAPTISTE JEANGÈNE VILMER, ALEXANDRE ESCORCIA, MARINE GUILLAUME & JANAINA HERRERA, INFORMATION MANIPULATION: A CHALLENGE FOR OUR DEMOCRACIES (2018), https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

113. *Id.* at 173.

Under European human rights law, these surveillance measures may impinge on the right to private life under Article 8 of the ECHR. The ECtHR has considered whether police violate a person's right to private life when they gather and retain information on a person's expressive public activity that is not illegal but may be concerning to authorities. In the 2019 judgment of *Catt v. the United Kingdom*,[114] an anti-war activist discovered he was included on a police extremism database, which documented information gathered by police about his presence at perfectly lawful protests. Following police refusal to delete the information from the database, the European Court ultimately found a violation of Article 8 of the ECHR. The Court was particularly critical of the police gathering of information based on the term "domestic extremism," which is not prescribed by law and which had a variety of working definitions.[115] The Court held that the police decision to "retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a 'chilling effect.'"[116] The Court reiterated that personal data "revealing political opinions attracts a heightened level of protection." It noted that there is "significant ambiguity over the criteria being used by the police to govern the collection of the data in question" and that "perhaps as a result, the database in issue appears to have been assembled on a somewhat ad hoc basis."[117]

Disinformation is similarly an ambiguous notion, which is in many instances not prescribed by law, and the ECtHR has long held that the "mere storing of information" on a person by the authorities amounts to an interference with the right to private life.[118]

B. Government Access to User Data

While access to platform data is advocated as an important tool to understand the distribution of disinformation, such access to user data could carry serious risks to user privacy. Specific attention is warranted for the inclusion of access-to-data provisions in new laws targeting disinformation. This issue raised its head during the passage of laws such as Germany's Network Enforcement Act in 2017[119] and France's Law on combatting the manipulation of information.

---

114. Catt v. United Kingdom, App. No. 43514/15, Eur. Ct. H.R. (2019), http://hudoc.echr.coe.int/eng?i=001-189424.

115. *Id.* ¶ 97.

116. *Id.* ¶ 123.

117. *Id.* ¶ 97.

118. *Id.* ¶ 93.

119. Netzwerkdurchsetzungsgesetz [NetzDG] [Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)], Oct. 1, 2017 (Ger.), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.

We turn first to Germany's Network Enforcement Act, which was enacted, according to the German government, in order to not only tackle hate speech but the "spread of 'fake news.'"[120] The Act operates as follows: section 3(1) places an obligation on platforms to maintain an "effective and transparent procedure for handling complaints about unlawful content" and must "supply users with an easily recognisable, directly accessible and permanently available procedure for submitting complaints about unlawful content."[121] Unlawful content is defined as content criminalized under twenty-two criminal offences under the German Criminal Code. Section 3(2) then sets out how platforms must operate their procedures for handling reports of unlawful content. First, platforms must take "immediate note" of any complaint and check "whether the content reported in the complaint is unlawful and subject to removal or whether access to the content must be blocked."[122] Second, and crucially, platforms must remove or block access to "content that is manifestly unlawful within 24 hours of receiving the complaint."[123] The Act does not define "manifestly unlawful."

While these provisions raise freedom of expression concerns, certain additional provisions raise right to privacy concerns.[124] The UN Special Rapporteur on freedom of expression raised right to privacy concerns during the passage of the Act. First, there was concern over the provision that mandated "storage and documentation of data concerning violative content and user information related to such content, especially since the judiciary can order that data be revealed."[125] The

120. *See* Letter from the Federal Government of Germany to the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (June 1, 2017), https://www.ohchr.org/Documents/Issues/Opinion/Legislation/GermanyReply9Aug2017.pdf; *see also* Amélie Heldt, *Reading Between the Lines and the Numbers: An Analysis of the First NetzDG Reports*, 8(2) INTERNET POL'Y REV. 1 (2019); Rebecca Zipursky, *Nuts About Netz: The Network Enforcement Act and Freedom of Expression*, 42 FORDHAM INT'L L. J. 1325 (2019); Heidi Tworek & Paddy Leerssen, An Analysis of Germany's NetzDG Law (Transatlantic High Level Working Grp. on Content Moderation Online & Freedom of Expression, Working Paper, 2019).

121. Access Now, *supra* note 106.

122. Netzwerkdurchsetzungsgesetz [NetzDG] [Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)], Oct. 1, 2017, § 3(2) (Ger.).

123. *Id.*

124. *See* ARTICLE 19, GERMANY: THE ACT TO IMPROVE ENFORCEMENT OF THE LAW IN SOCIAL NETWORKS (2017), https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf ("[T]he Act expands the list of grounds on which law enforcement can request users inventory data from 'service providers.' This new ground includes inventory data 'necessary for the enforcement of civil law claims arising from the violation of absolutely protected rights by unlawful content as defined in the Network Enforcement Act.'"); *see also* MATTHIAS C. KETTEMANN, FOLLOW-UP TO THE COMPARATIVE STUDY ON "BLOCKING, FILTERING AND TAKEDOWN OF ILLEGAL INTERNET CONTENT" (2019), https://rm.coe.int/dgi-2019-update-chapter-germany-study-on-blocking-and-filtering/168097ac51.

125. David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, at 5, U.N. Doc. OL/DEU/1/2017 (June 1, 2017).

Special Rapporteur stated that this could "undermine the right individuals enjoy to anonymous expression," and these

> restrictions on anonymity, in particular absent judicial oversight, facilitate State surveillance by simplifying the identification of individuals accessing or disseminating prohibited content. By requiring complaints and measures to be documented and stored for an undisclosed amount of time, without providing further protection mechanisms against the misuse of such data, individuals become more vulnerable to State surveillance. These provisions also allow for the collection and compilation of large amounts of data by the private sector, and place a significant burden and responsibility on corporate actors to protect the privacy and security of such data.[126]

Second, the Special Rapporteur was concerned with the

> possibility that users claiming a violation would be entitled to be given access to subscriber data without prior court approval. The protection of anonymity, including protection against unlawful and arbitrary interference by state or non-state actors, plays a critical role in securing the right to freedom of opinion and expression. The absence of a judicial warrant for the disclosure of individual information would represent a restriction that is neither targeted nor protecting of due process rights, and it would therefore not meet the strict test required for restrictions on privacy and expression.[127]

The German government responded that the Rapporteur's "concerns of providing access to subscriber data without prior court approval have been met by introducing the requirement of a court decision prior to surrendering personal data."[128] Yet, in 2020, the German government made further amendments to the NetzDG Act by passing a law intended to combat right-wing extremism. This law requires that platforms send suspected criminal content directly to the federal police at the time it is reported by a user.[129]

Similarly, in France, there has been movement toward increased access to user data. In 2019, the French government announced that for the first time ever,

---

126. *Id.*

127. *Id.*

128. Letter from the Federal Government of Germany to the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *supra* note 119, at 2.

129. *See* DEUTSCHER BUNDESTAG, GESETZ GEGEN RECHTS-EXTRE-MISMUS UND HASS-KRIMI-NA-LITÄT BESCHLOSSEN [Law Against Right-Wing Extremism and Hate Crime Passed] (June 18, 2020) (Ger.), https://www.bundestag.de/dokumente/textarchiv/2020/kw25-de-rechtsextremismus-701104; Philipp Grüll, *German Online Hate Speech Reform Criticised for Allowing 'Backdoor' Data Collection*, EURACTIV (June 19, 2020), https://www.euractiv.com/section/data-protection/news/german-online-hate-speech-reform-criticised-for-allowing-backdoor-data-collection; Natasha Lomas, *Germany Tightens Hate Speech Rules to Make Platforms Send Reports Straight to the Feds*, TECHCRUNCH (June 19, 2020, 7:02 AM), https://techcrunch.com/2020/06/19/germany-tightens-online-hate-speech-rules-to-make-platforms-send-reports-straight-to-the-feds.

Facebook had agreed to hand over identification data of French users suspected of posting hate speech on its platform to judges.[130] Previously, Facebook had only cooperated on matters related to terrorism and violent acts by transferring the IP addresses and other identification data of suspected individuals to French judges. Notably, in relation to the 2018 Law on Combatting the Manipulation of Information, the UN Special Rapporteur raised concerns that the "cooperation mechanism established under Article 9 authorizes the Government to access the data of subscribers, related to the reported content, without prior court approval."[131] In particular, the "absence of a judicial authorization for the disclosure of personal information would be a restriction which is neither targeted nor protective of rights to a fair hearing and would therefore not meet the strict test for imposing restrictions on privacy and freedom of expression."[132]

Further, the French media regulator, *Conseil Supérieur de l'Audiovisuel* (CSA), adopted recommendations in 2019 under the 2018 Law on Combatting the Manipulation of Information, which "encourages" platforms to set up "appropriate procedures allowing for the detection of accounts disseminating false information on a massive scale."[133] The CSA also expressly states that it reserves the "ability [to] request[] any information should it observe a manipulation of information or an attempt to manipulate information likely to disturb public order or to affect the sincerity of an election."[134]

Outside of Europe, governments are going much further. Brazil's draft Fake News Law mandates that platforms maintain records of forwarded messages for a period of four months, which may be requested under a court order.[135]

---

130. *See* Mathieu Rosemain, *In a World First, Facebook to Give Data on Hate Speech Suspects to French Courts*, REUTERS (June 25, 2019, 7:23 AM), https://www.reuters.com/article/us-france-tech-exclusive/exclusive-in-a-world-first-facebook-to-give-data-on-hate-speech-suspects-to-french-courts-idUSKCN1TQ1TJ.

131. David Kaye (Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression), *Mandat du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression [U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion, and Expression]*, U.N. Doc. OL/FRA 5/2018, at 7 (May 28, 2018).

132. *Id.*

133. CONSEIL SUPÉRIEUR DE L'AUDIOVISUEL, RECOMMENDATION NO. 2019-03 OF 15 MAY 2019 OF THE CONSEIL SUPÉRIEUR DE L'AUDIOVISUEL TO ONLINE PLATFORM OPERATORS IN THE CONTEXT OF THE DUTY TO COOPERATE TO FIGHT THE DISSEMINATION OF FALSE INFORMATION, at § 4(a) (Fr.), http://www.csa.fr/content/download/254203/733091/version/1/file/CSA%20-%20Projet%20de%20recommandation%20aux%20op%C3%A9rateurs%202504_eng-GB.pdf.

134. *Id.*

135. *See Brazil: Reject "Fake News" Bill - Current Draft Violates Free Speech and Association, Privacy*, HUM. RTS. WATCH (June 24, 2020, 10:31 AM), https://www.hrw.org/news/2020/06/24/brazil-reject-fake-news-bill; Katitza Rodriguez & Seth Schoen, *5 Serious Flaws in the New Brazilian "Fake News" Bill That Will Undermine Human Rights*, ELEC. FRONTIER FOUND. (June 29, 2020), https://www.eff.org/deeplinks/2020/06/5-serious-flaws-new-brazilian-fake-news-bill-will-undermin e-human-rights.

C. The Use of Data Protection Law as a Shield by Platforms

While platforms are cooperating with governments in various initiatives to remove illegal and harmful content such as disinformation, platforms are simultaneously invoking data protection law concerns in response to recent efforts to increase transparency with respect to the function and impact of their systems. As mentioned above, access to platform data is widely considered a key mechanism in understanding the problems of disinformation, designing policy responses, and assessing platform responses. However, platforms have strong incentives, apart from data protection law, to keep their systems closed, including to maintain their dominant position in the market, where data are highly valuable.[136] As Inge Graef, Sih Yuliana Wahyuningtyas, and Peggy Valcke argue, maintaining concentration and lack of access to data creates barriers for competitors and new entrants.[137]

There is tension in the EU Code of Practice on disinformation regarding access to data. The Code contains, as mentioned earlier, a pillar on platforms providing privacy-compliant access to data for research activities and for platforms to "cooperate by providing relevant data on the functioning of their services including data for independent investigation by academic researchers and general information on algorithms."[138] However, there has been a tension between the expectation under the Code for the facilitation of access to data and how it has played out in practice. Following its first year of operation, the European Commission commented that the provision of data to the research community was "episodic and arbitrary" and noted that platforms "generally cite alleged risks of data protection violations as inhibiting cooperation with the research community."[139] Similarly, in platform submissions on the operation of the Code, platforms such as Facebook admitted that "many stakeholders are eager for data to be made available as quickly as possible," while adding that it was "committed to taking the time necessary to incorporate the highest privacy protections and building a data infrastructure that provides data in a secure manner."[140]

As such, there is growing frustration in European policy circles over the (strategic) attempts to leverage vague data protection law concerns. ERGA's report on the operation of the Code's data-access provision "show[s] clearly that the platforms provided very little (if any) access to data for independent

136. *See* Inge Graef, Sih Yuliana Wahyuningtyas & Peggy Valcke, *Assessing Data Access Issues in Online Platforms*, 39 TELECOMM. POL'Y 375 (2015).

137. *Id.* at 385.

138. EU CODE OF PRACTICE, *supra* note 27, § II.E.

139. *See* Eur. Comm'n, *Code of Practice on Disinformation: First Annual Reports*, at 12 (Oct. 2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62698.

140. *See Facebook Report on the Implementation of the Code of Practice for Disinformation*, § 5.1, (Sept. 2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62681.

investigation."[141] Platforms argue "that they cannot provide free[] access to data because of privacy and data security reasons, but these reasons are not fully convincing."[142] This skepticism of the data-protection justifications put forward by platforms led ERGA to call upon platforms to "provide formal analyses identifying their specific concerns regarding data sharing for independent academic research under" the General Data Protection Regulation (GDPR).[143] ERGA hoped that such analyses would provide a "starting point for resolving areas of ambiguity and uncertainty."[144] ERGA also called on data protection authorities to "offer formal guidance on permissible data sharing practices under GDPR."[145] Scholars are also skeptical of the data protection concerns put forward by platforms and in response are providing models for access to data based on the relevant experience of other sectors, such as health-data research.[146]

The proposed Digital Services Act on reforming the EU's rules in relation to platforms contains substantive new rules on access to data.[147] An important part of the proposed legislation is the creation of new dedicated regulatory bodies, which would be empowered to access data from large online platforms and to gain insights into their business practices and the impact on users. Indeed, large platforms would also be obliged to provide data access to certain "vetted researchers" in order to conduct research that "contributes to the identification and understanding of systemic risks" associated with platforms,[148] including intentional manipulation of platforms' services and the inauthentic use or automated exploitation of their services.[149]

III. DATA PROTECTION LAW AS A STRUCTURAL SAFEGUARD

In the previous two Parts, we reviewed the various ways in which disinformation policy can be a threat to the fundamental rights to privacy and freedom of expression. At the same time, privacy law and, in particular, data protection law currently provide the main systemic regulatory safeguards in Europe in relation to disinformation. However, before expanding upon the structural

141. *ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice*, at 49 (2020), https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.

142. *Id.* at 40.

143. *Id.*

144. *Id.*

145. *Id.*

146. *See* JEF AUSLOOS, PADDY LEERSSEN & PIM TEN THIJE, OPERATIONALIZING RESEARCH ACCESS IN PLATFORM GOVERNANCE: WHAT TO LEARN FROM OTHER INDUSTRIES? (2020), https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf.

147. *Regulation of the European Parliament an of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*, *supra* note 30, at 63–63.

148. *Id.*

149. *Id.* at 59–60.

safeguards provided by data protection law, many other structural safeguards for guaranteeing a pluralistic public debate and media environment existed in Europe, particularly around guaranteeing pluralism of viewpoints during election-time. Most EU member states still heavily regulate broadcast media by imposing many rules on broadcaster (both public and private) impartiality, fairness, and accuracy.[150] During election-time, many EU member states prohibit paid-for political advertising on television. In countries such as Italy, a specific election law ("*Par Condicio*" Law) regulates election-time political communication across the press, broadcast, and online, with rules on media coverage of candidates, politicians, and political parties to ensure fairness and equal coverage.[151] Further, EU member states regulate media reporting of opinion polls, exit polls, election debates, and impose silence periods in the run-up to polling day. Indeed, these rules came into play during the 2017 French presidential election: just as the silence period was coming into effect, nine gigabytes of presidential candidate Emmanuel Macron's confidential campaign documentation were published online. However, the French Presidential Election Commission (CNCCEP) issued a strongly worded statement on the eve of the election, urging both traditional media and online media to refrain from reporting on the content of the leaks. Indeed, French media generally heeded the call[152] in the interests of ensuring free expression of the opinion of the people and the "sincerity of the vote."[153]

In addition to the aforementioned structural framework, data protection law also protects online users' autonomy in relation to data-driven campaigns. Data protection law requires transparency for internet audiences about targeting and offers data subject rights in relation to audience platforms, such as social media companies that monetize social services in ways that create new avenues for audience targeting.

It's on this last aspect—the way that communications end up being disseminated on social media and other channels—that EU data protection law has the most potential. EU data protection law applies to the processing of personal data, which are defined as any information relating to an identified or identifiable individual (natural person). This law requires transparency and a lawful basis such as consent. It also grants rights to access, correction, and deletion for data subjects,

150. *See* Anette Alén-Savikko, Ernesto Apa, Marco Bassini, Francisco Javier Cabrera Blázquez, Ingrid Cunningham, Christina Etteldorf, Agnès Granchet, Beata Klimkiewicz, Ronan Ó Fathaigh, Juraj Polák, Tony Prosser, Andrei Richter & Nathalie Rodriguez, MEDIA REPORTING: FACTS, NOTHING BUT FACTS? (2018).

151. *See* ERNESTO APA & MARCO BASSINI , *Italy*, *in* MEDIA COVERAGE OF ELECTIONS: THE LEGAL FRAMEWORK IN EUROPE (2017).

152. Rachel Donaldio, *Why the Macron Hacking Attack Landed With a Thud in France*, N.Y. TIMES (May 8, 2017), https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html.

153. Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle, *Recommandation aux médias suite à l'attaque informatique dont a été victime l'équipe de campagne de M. Macron* [*Recommendation to the Media Following the Computer Attack Against Mr. Macron's Campaign Team*] (May 6, 2017), http://www.cnccep.fr/communiques/cp14.html.

all of which are subject to independent regulatory oversight. As personal data are likely to be a key ingredient to disinformation campaigns and strategies, data protection law will apply to the actors who are steering the messaging and campaigns, as well as the services, such as social media platforms, that provide a platform for data-driven communications. By putting a check on what is happening with personal data in the online domain, data protection law has the potential, at least in theory, to be an important safeguard.

Areas in which data protection law and disinformation have intersected for quite some time are the use of personal data, predictive analytics, and behavioral targeting in elections. As the European Data Protection Board (EDPB) puts it in its recent guidance on elections, "Compliance with data protection rules, including in the context of electoral activities and political campaigns, is essential to protect democracy."[154] The EDPB notes that for targeted messaging "adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it and how they can exercise their rights as data subjects."[155] It further notes the fact that voter data and personal data that reveal political opinions is considered a "special category" of data, which will generally require the explicit consent of the individual to be used by third parties.[156] It clarifies that personal data that has been made public, such as the information on someone's social media profile, falls within the scope of the regulation and cannot be collected and processed without constraints. Finally, the guidance also highlights the special protections of people against profiling and automated decision-making. In this context, it notes that "profiling connected to targeted campaign messaging may in certain circumstances cause 'similarly significant effects' and shall in principle only be lawful with the valid explicit consent of the data subject."[157]

The most thorough guidance on the topic was released by the European Data Protection Supervisor in its *Opinion on online manipulation and personal data*.[158] The Opinion covers a broad range of concerns around online manipulation (and the data-driven strategies underpinning new forms of manipulation). Notably, the context of disinformation and related strategies are of central concern to the EDPS. The EDPS considers online manipulation to be a symptom of a broader lack of accountability in the digital ecosystem. It calls for robust enforcement of existing data protection rules, together with other norms on elections and media pluralism

154. European Data Protection Board Statement 2/2019, Statement on the Use of Personal Data in the Course of Political Campaigns (Mar. 13, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

155. *Id.* at 2.

156. *Id.*

157. *Id.*

158. *Opinion of the European Data Protection Supervisoron Online Manipulation and Personal Data*, Opinion 3/2018 (Mar. 19, 2018), https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

in view of the threats to fundamental rights and the functioning of democracy. The European Commission notes in its recent evaluation of the GDPR, "protecting personal data is . . . instrumental in preventing the manipulation of citizens' choices, in particular via the micro-targeting of voters based on the unlawful processing of personal data, avoiding interference in democratic processes and preserving the open debate, the fairness and the transparency that are essential in a democracy."[159]

As pointed out by others, disinformation campaigns may involve the profiling of audiences with regard to their susceptibility to being misled by certain communications.[160] In other words, whereas a certain susceptibility with respect to disinformation may exist, it's the data-driven profiling and targeting that creates significant additional challenges. While some have proposed curtailment of the granularity of targeting possibilities in the context of political messaging, perhaps a similar result could be reached through strict enforcement of data protection rules with respect to political campaigns in Europe.

CONCLUSION

This Article has focused on the problematic aspects of European disinformation policy, particularly relating to overbroad content-based restrictions, law enforcement involvement, and increased monitoring of the online environment. However, another important strand of European disinformation policy is being developed under the European Democracy Action Plan adopted in late 2020.[161] Crucially, the Democracy Action Plan, as distinct from upcoming regulation of online platforms under the DSA, seeks to tackle disinformation through measures such as funding projects to support deliberative democratic infrastructures, strengthening media freedom and media pluralism, and strengthening empowerment of citizens to make informed decisions through strengthening media literacy.[162] This framework is consistent with the ECtHR's holding that states not only have a negative duty of non-interference with freedom of expression, but also have a "positive obligation" to put in place an appropriate legislative and administrative framework to guarantee effective pluralism[163] and "create a favourable environment for participation in public debate by all the persons

159. *Commission Communication to the European Parliament and the Council on Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation*, at 4, COM (2020) 264 final (June 24, 2020).

160. *See* Karen Kornbluh, *Could Europe's New Data Protection Regulation Curb Online Disinformation?*, COUNCIL ON FOREIGN RELATIONS (Feb. 20, 2018), https://www.cfr.org/blog/could-europes-new-data-protection-regulation-curb-online-disinformation.

161. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – On the European Democracy Action Plan*, *supra* note 8.

162. *Id.* at 9, 11, 24. European Democracy Action Plan - Roadmap, Ref. Ares (2020)3624828 (July 9, 2020).

163. Centro Europa 7 S.r.l. v. Italy, App. No. 38433/09, 2012-III Eur. Ct. H.R. 267, 310 (2012).

concerned."[164] The Democracy Action Plan would align with international freedom of expression standards, which emphasize that a key means of addressing disinformation is for states to promote a free, independent, and diverse communications environment, including media diversity.[165]

164. Huseynova v. Azerbaijan, App. No. 10653/10, Eur. Ct. H.R. 23 (2017).

165. *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*, *supra* note 95, at § 3(a).