Brutti N, 'Tortious disinformation and digital platforms' (2025) 1 EJPLT.
DOI: https://doi.org/10.57230/EJPLT251NB

EJPLT
ISSN 2704-8012



Tortious disinformation and digital platforms

Disinformazione dannosa e piattaforme digitali

NICOLA BRUTTI
Associate Professor of Comparative Private Law
University of Padua

Abstract

The spread of false and harmful speech has always existed but it has often fallen within the protection afforded to freedom of expression as a fundamental right. In the Internet era, extending civil liability to digital platforms for the dissemination of unlawful contents has always been regarded with skepticism and disfavor, also because of the potential chilling effect. Since the dissemination of dangerous fake news has been increasing in recent years, the idea of preventing them through an expansion of torts has gained ground. As a part of EU soft law (COM(2018) 236 final), a "catch-all provision" focuses on instrumentalizing the spread of disinformation for profit purposes. To this extent it should be noted that the most serious threat does not depend so much on the peculiar content disseminated, but rather on the algorithm that govern digital platforms. The EU "Digital Services Act" (DSA) tries to cope with such complex issue, enhancing a co-regulatory approach in order to mitigate this technological and systemic risk. If the DSA opts mainly for public enforcement, on the other hand it still acknowledges the coexistence of civil liability, which could derive precisely from a breach of cooperation duties and would recall the interpretative value of the aforesaid "catch-all provision".

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
*La diffusione di discorsi falsi e dannosi è un fenomeno da sempre esistito, ma spesso rientra nell'ambito della tutela garantita alla libertà di espressione, quale diritto fondamentale. Nell'era di Internet, l'estensione della responsabilità civile alle piattaforme digitali per la diffusione di contenuti illeciti è stata tradizionalmente accolta con scetticismo e sfavore, anche a causa del possibile effetto dissuasivo ("*chilling effect*"). Tuttavia, poiché negli ultimi anni si è registrato un incremento nella diffusione di* fake news *pericolose, si è affermata progressivamente l'idea di prevenirle mediante un ampliamento delle fattispecie illecite in ambito extracontrattuale. Nell'ambito della* soft law *dell'Unione Europea (COM(2018) 236 final), una clausola di tipo generale ("*catch-all provision*") si concentra sulla strumentalizzazione della disinformazione a fini di lucro. A tal proposito, occorre rilevare che la minaccia più grave non risiede tanto nel contenuto specifico diffuso, quanto piuttosto negli algoritmi che regolano il funzionamento delle piattaforme digitali. Il* "Digital Services Act" *(DSA) dell'UE affronta tale questione complessa mediante un approccio co-regolatorio, volto a mitigare tale rischio tecnologico e sistemico. Sebbene il DSA privilegi principalmente l'enforcement pubblico, esso riconosce, tuttavia, la coesistenza di una responsabilità civile, la quale può derivare da una violazione degli obblighi di cooperazione e richiama, in tal senso, il valore interpretativo della suddetta clausola generale.*

Keywords: Fake news; Disinformation; Free Speech; Social Networks; Digital Services Act; Defamation; Systemic Risk; Co-regulation; Civil Liability

Summary: 1. 'Fake news' and freedom of expression. – 2. The EU approach to "online disinformation" as a soft law instrument. – 3. Algorithm-amplified disinformation and systemic risk. – 4. Cooperation duties and the role of the EU Commission.

1. 'Fake news' and freedom of expression.

Online disinformation is one of the issues that has caused great concern in recent years, with particular reference to large search engines and social networks. The severity of such risks became clear during the recent pandemic and in the 2020 US presidential election. On the other hand, France and Germany had already adopted legislation specifically aimed at obtaining rapid feedback from platforms in the event of reports of news aimed at spreading discredit and political hatred against minority groups and democratic institutions. [1] In particular, the French law (*Loi contre la manipulation de l'information* [2]) was born from the need to control the use of robotized

[1] See *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Netz DG) - «Law of 1 September 2017 on the enforcement of networks (Federal Official Gazette I p. 3352), last amended by Article 29 of the Law of 6 May 2024 (Federal Official Gazette 2024 I no. 149)- conceived precisely to counter the wave of far-right hate speech, artificially fomented by fake news spread on social networks (in particular, Facebook).

[2] Law n. 2018-1202 of 22 December 2018. Among the most significant legal cases: *TGI Paris, 17 mai 2019, n° 19/53935*: the court considered that "while the message written by Mr. Christophe Castaner appears exaggerated in that it mentions the term attack and injuries, this exaggeration relates to facts that are real, namely the intrusion of demonstrators into the grounds of the Pitié-Salpêtrière hospital on May 1, 2019." The information is therefore not without any link with real facts and the allegation is not "manifestly inaccurate or misleading." (case note by Pierre Januel, Marine Babonneau, 'Loi Fake news : première application du référé', *Dalloz Actualité. Le quotidien du droit*, (21 May, 2019); *Tribunal correctionnel de Paris,*

information on social networks (social bots) for electoral propaganda, fearing interference from foreign States. Both measures have raised criticism and opposition, especially from platforms, due to the short time left to them to act and the very heavy sanctions envisaged in the event of delays or omissions.[3] Among the most recent events, we can highlight the blocking of the social network "X" by the Brazilian Supreme Court (30 August 2024)[4]. The latter stated that the owner, Elon Musk, had supported the systematic dissemination of fake news and political hate speech and thus he was responsible of malicious instrumentalization of social networks for criminal purposes[5]. Jurists are nowadays faced with new concepts that are difficult to trace back to consolidated legal categories. In fact, it has been highlighted that 'fake news' and 'disinformation' are expressions unknown in legal language, belonging, more properly, to 'journalistic jargon'.[6] In these pages, I will try to explain how the theme of countering disinformation is nothing new; on the contrary, it is well known in legal systems, even if it is dealt with in a fragmentary way and with various facets. At the same time, information technologies are undergoing an extraordinary acceleration that quickly makes regulation obsolete. Therefore, with the emergence of phenomena in many ways distant from those of the past, this pre-existing framework may appear inadequate. For this reason, it is worth reflecting and developing conceptual formulas and legal disciplines, which are more useful for dealing with new risks.

Thinking of a question provocatively posed by Ronald Coase: if information competes in the free market of ideas, why should it not be regulated, like any other commodity or service, to avoid failures of that same market?[7] Freedom of expression, however, constitutes an inalienable fundamental right of the person and it is extremely difficult to regulate or classify its contents, like any consumer good or commodity. Above all, the idea of relying on automated classification systems, which involve a sort of oppressive labeling of information, is a cause for concern.[8]

In modern democracies, a central role is assigned to the free expression of thought, incompatible with any test of truth. The US experience provides an

---

12 septembre 2024: two women were founded liable (defamation) for having spread the rumor that Brigitte Macron was a transgender woman (see 'Infox sur Brigitte Macron femme transgenre : deux femmes condamnées', *Le Figaro* 12 September, 2024); *Tribunal correctionnel de Senlis, 2 novembre, 2020*: the Senlis Criminal Court found the author of a false video- posted on March 17, 2020 and claiming that the Pasteur Institute had invented Covid-19- liable for public defamation against the Pasteur Institute (https://www.pasteur.fr/fr/journal-recherche/actualites/covid-19-tribunal-correctionnel-senlis-condamne-diffamation-auteur-video-fake-news).

[3] For critical references also to the German experience, D de Bellescize, 'Fake news: une loi polémique, qui pose plus de questions qu'elle n'en résout' (2018) 4 *Constitutions* 559-570.

[4] The original and full version of the decision, *Pet. 12.404/DF*, can be found in attachment to the article by T Angelo, 'Alexandre de Moraes determina bloqueio do X no Brasil', *ConJur-Consultor Jurídico* (30 August 2024) (http://www.conjur.com.br/2024-ago-30/alexandre-de-moraes-determina-bloqueio-do-x-no-brasil/).

[5] See *Pet. 12.404/DF* (n 5) 17.

[6] See V Zeno-Zencovich, 'The EU Regulation of Speech. A Critical View' (2023) 1 Media Laws 5-6.

[7] See A Nicita, *Il mercato delle verità. Come la disinformazione minaccia la democrazia* (Il Mulino, 2021) 203 quoting R H Coase, 'The market for goods and the market for ideas' (1974) 64 (2) American Economic Review 384-391.

[8] See Vincenzo Zeno-Zencovich, *The EU Regulation* (n 7) 1: "expression is seen not as a freedom – in the sense we have forged this notion over the centuries, and in particular over the last two centuries – but a regulated activity, similar to the production of goods or the provision of services.".

emblematic case of constitutionally protected freedom of expression.[9] In fact, the first amendment makes it a milestone of advanced democratic systems. Metaphorically imagining a free market of opinions, Judge Oliver Wendell Holmes affirmed, in a famous dissenting opinion of 1919, that the goal of truth is best pursued through the free trade of ideas.[10] So the idea of strict legislation on disinformation is not convincing. In fact, limitations on freedom of expression risk becoming censorship, if not punctually substantiated in cases of serious threats to interests equally worthy of protection. In certain cases, some limitations on freedom of expression are not only appropriate, but necessary. Again, Justice Holmes, resorting to another imaginative metaphor and thus outlining the pioneering "clear and present danger test", warned that free speech cannot be guaranteed when someone falsely shouts "fire!" in a crowded theater, causing panic.[11]

Especially in the post-war German constitutional experience, there is also a tendency to attribute to other rights of the person, especially dignity, the ability to counterbalance freedom of expression.[12] Think about tort of defamation, damage to reputation, but also of more disputed rules about 'publication or dissemination of false, exaggerated or tendentious news' (e.g. art. 656 of the Italian Criminal Code).[13] Furthermore, with post-industrial development, the number of disciplines aimed at promoting better quality and correctness of information has progressively expanded. Beyond the laws on the press, which entail gatekeeping positions and control obligations, one can mention other examples: i. the standards of journalistic conduct; ii. corporate governance and financial transparency; iii. access to information in the public sector (e.g. freedom of information act, access to environmental information); iv. Consumer's right to be correctly informed on safety, health and

[9] In a comparative perspective, see: W Brugger, 'Bans On or Protection of Hate Speech? Some Observations Based on German and American Law', (2002) 17 Tulane European and Civil Law Forum 3-4, 15-16, where the differences between German and American Law emerge plastically in the treatment given to the Holocaust denial theses and the apologia of Nazism (p. 15); and, for an effective synthesis, M Luciani, *La libertà di espressione, una prospettiva di diritto comparato* (EPRS, European Parliament Research Service, 2019) 18; A Baldassarre, *Privacy e Costituzione. L'esperienza statunitense* (Bulzoni, 1974) 178.

[10] Justice Holmes found in that case that, although the defendant had disseminated harshly critical ideas about the US government's intervention in World War I, as well as protests against increased military spending, this did not constitute a conspiracy against United States, punishable under the *Espionage Act* of 1917. See *Abrams v. United States*, 250 U.S. 616 (1919). The expression "free market place of ideas", already in essence in Holmes' speech, was coined later, in the case *United States v. Rumely* 345 U.S. 41 (1953), by Justice Douglas. See R Coase, 'Markets for Goods and Market for Ideas' (1974) 64(2) American Economic Review 384.

[11] See *Schenck v. United States*, 249 U.S. 47, 52 (1919), on which cf. Leslie G. Jacobs, 'Freedom of Speech and Regulation of Fake News', (2022) 70 The American Journal of Comparative Law 292; Carlton F.W. Larson, 'Shouting 'Fire' in a Theater: The Life and Times of Constitutional Law's Most Enduring Analogy', (2015) 24 Wm. & Mary Bill Rts. J 181.

[12] Some have highlighted a risk of dehumanization of the person, faced with the decision-making substitution of the algorithm: Stefano Rodotá, 'Antropologia dell'"homo dignus"', in G Alpa and M R Marella (eds.), *Critica del diritto privato. Editoriali e saggi della Rivista Critica del Diritto Privato*, (Jovene 2017) 352; G Resta, *'Capitolo 5. La dignità'*, in *Trattato di biodiritto diretto da* P Zatti, S Rodotá*, Ambito e fonti del biodiritto*, (eds. S Rodotá and M Tallacchini (Giuffrè 2010) 259.

[13] About such limitations, V Zeno-Zencovich, *La libertà d'espressione, Media, mercato, potere nella società dell'informazione*, (Il Mulino 2004) 119-120. The art. 656 of the Italian criminal code provide a "crime of pure danger" for the existence of which it is not relevant "the fact that no disturbance of public order has occurred, it being sufficient that there was an abstract possibility that such a disturbance in effects were to occur" (Criminal Court of Cassation, Section I, sentence no. 9475 of 7 November 1996). Cf. S Latorre, 'Fake News: la pubblicazione di notizie false' (5 December 2021) http://lamagistratura.it.

environmental issues in advertising communications, including the 'greenwashing' issue.[14] Considering their specificity, these rules represent not so much a perspective of public censorship, but rather the result of inclusive and participatory policies, so as to theorize a more general right to be informed, as an element of citizenship.[15]

Given the aforementioned examples, we can agree that freedom of expression has been transformed, over time, from an exclusively negative freedom (the right not to be subject to censorship interference by public authority), into a positive freedom (the right to have correct information, at least in certain areas).[16] Of course, this sparks a debate about the meaning and scope of free speech today, given a profoundly transformed media system.[17] One of the main objectives of EU Digital Services Act (DSA) is to harmonize "diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online disinformation or other societal risks".[18]

2. The EU approach to "online disinformation" as a soft law instrument.

If there has always been a difficulty in assimilating the hosting activity of very large online platforms (VLOP) to publishers, [19] on the other hand it does not seem plausible to limit its responsibilities to those of a simple carrier, due to

[14] For example, see A P J Mol, 'Environmental governance in the Information Age: the emergence of informational governance' (2006) 24 (4) Environment and Planning C Government and Policy 497-514; C R Sunstein, 'Informational Regulation and Informational Standing: Akins and Beyond', (1999) 147 U. Pa. L. Rev. 615. Regarding misleading advertising and unfair commercial practices, recent jurisprudence has recalled that the legal basis of consumer protection is to be found in art. 153 of the EEC founding Treaty, as a precursor of today's art. 169, TFEU according to which in order to promote the interests of consumers and ensure a high level of consumer protection, the Union contributes to protecting the health, safety and economic interests of consumers as well as to promoting their right to information, education and organization for the protection of one's interests. It was highlighted that as well as the Greenwashing phenomenon expands, there is the convergence of a plurality of regulatory subjects and reference regulations, all functional to the objective of guaranteeing compliance with a general principle of truth of the message which also has an advertising nature.». See Ord. Trib. Gorizia, 25 November 2021 (Judge Dr. F. Clocchiatti), https://www.dirittobancario.it/art/greenwashing-primi-orientamenti-giurisprudenziali/. See also: L Evans, 'The Green Claims Directive: The Future Legal Framework for Advertising with Environmental Claims' (2024) 19 Eur Food & Feed L Rev 174.

[15] Cf. V Zeno-Zencovich, 'Il diritto ad essere informati quale elemento del rapporto di cittadinanza' (2006) 1 Dir inf 1-10.

[16] A key to understanding free speech based on the search for truth, beyond the mere external non-interference, dates back to J Stuart Mill, *On Liberty*, 43-44 (Elizabeth Rapaport ed., Hackett Publ'g Co. 1978) (1859); T I Emerson, 'First Amendment Doctrine and the Burger Court'(1980) 68 Calif L Rev, 422, 423 and, more recently, S G Gey, 'The First Amendment and the Dissemination of Socially Worthless Untruths', (2008) 36 *Fla. St. U. L. Rev.* 1, 3; H Norton, *Distrust, Negative First Amendment Theory, and the Regulation of Lies* (Knight First Amendment Institute at Columbia University 2022).

[17] See R A Cass, 'The Perils of Positive Thinking: Constitutional Interpretation and Negative First Amendment Theory' (1987) 34 UCLA L Rev 1405, 1412; G Lakier, 'The First Amendment's Real Lochner Problem' (2020) 87 U Chi L Rev 1243, 1332; J M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 N.Y.U. L. Rev. 1, 3–4 (freedom of expression must not be separated from the actual possibility of participating democratically in public debate); M Lavi, 'Do Platforms Kill?' (2020) 43(2) Harv Journ of Law & Public Policy 526; H Micklitz *et al.* (Eds.), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2022).

[18] See Recital no. 2, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[19] Cf. W Oremus, 'How social media 'censorship' became a front line in the culture war' (*The Washington Post*, October 9, 2022).

the huge interferences on the content conveyed. Think of moderation actions, the possibility of filtering illegal content, now enhanced by the use of artificial intelligence.

In the US model, the priority is evidently not to penalize the development potential of the Internet ("chilling effect") and to highlight the value of free speech. Thus, the notice and take down procedure is essentially limited to copyright protection, leaving the fight against other wrongful acts to the provider's free choice, through the 'Good Samaritan Clause'.[20] This relegates content moderation policies and prevention measures to the discretionary power of providers, protecting them from liability.

In the EU, on the other hand, from an initially pro-neutral approach we have gradually move to the less favorable case-law on active hosting.[21] Although the Digital Services Act confirms that it does not impose general control duty on platforms, thus immunizing them from strict liability (art. 6), there is an obligation to act, as soon as such violations become known. In this way, the notice and take down system, already established for copyright infringements in the US model, is consequently expanded.[22]

The many opportunities created by the massive, and sometimes chaotic, dissemination of information on the Internet has also led to the proliferation of harmful content. Given the danger of the spread of fake news on the internet, the EU elaborates the concept of "online disinformation", as emerges in the EU Commission's Communication "Tackling online disinformation: a European approach" (COM/2018/236)[23], and also in the EU Report, "A Multi-dimensional approach to disinformation" of 2018, recalled in the preamble of the enhanced Code of Practice on Disinformation (2022). Due to such a provision, "online disinformation" must be objectively false or misleading, conceived and then disseminated (design, presentation and promotion of content) for profit purposes or to intentionally deceive the public. A further requirement is then mentioned: it may cause public harm, that comprises

[20] Think of Section 230, *Communications Decency Act* (CDA) 1996, see J Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).

[21] See, among many, E Andreola, 'Fake news e danno da false informazioni in internet - II Parte' (2020) 6 Resp civ prev, 2002 and the case-law cited therein. In the case "Glawischnig-Piesczekc. Facebook Ireland" C-18/18, decision on a preliminary ruling of 3 October 2019, taken on the basis of Directive 2000/31/EC, the Court of Justice of the EU stated that the court of a Member State may order the hosting provider to remove information stored with content equivalent to other information previously declared illegal and extend the effects of the injunction worldwide. However, it also clarified that hosting service providers are not subject to a general obligation to monitor the information they transmit or store, just as they do not have a general obligation to actively seek out illegal comments (2020) 3 Dir ind, 284-285, case note by E Tosi, 'Obblighi di filtraggio "ex post" di contenuti digitali illeciti equivalenti e responsabilità civile degli "hosting provider"'. The Court's decision has also been quoted by *Tribunale di Roma, Sentenza n. 17909,* 5 December 2022 (*Casapound Italia v Facebook*), (2023) 2 Dir inf, 245, commented by B Mazzolai, '"Hate speech" e comportamenti d'odio in rete. "Casapound vs Facebook": atto III'.

[22] See V Zeno-Zencovich, 'The EU Regulation' (n 7), who, with regard to the initial exclusion of liability referred to in art. 6, highlights: «these rules are set aside by the subsequent art. 16 which mimics the "notice and take-down" procedures common to online copyright infringement.»

[23] Par. 2.1 (3-4): "Disinformation is understood 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. Public harm comprises threats to democratic political and policy making processes as well as public goods such as the protection of EU citizens' health, the environment or security. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary. This Communication is without prejudice to the applicable legal rules at Union or national level relating to the issues discussed, including disinformation containing illegal content.".

threats to democratic political and policy making processes as well as public goods such as the protection of EU citizens' health, the environment or security. Wrongs already provided for by other laws, such as defamation, are excluded, as well as all those manifestations, such as satire and parody or clearly partisan political communications which, in a self-evident way, are outside the news function. [24] Such a broad definition almost seems to expand the tort of defamation so as to include any false or misleading information capable of causing public harm, thus resembling to a "catch-all provision". The reference to the purpose of profit, as a requirement for considering disinformation illegal, seems to refer to the behavior of big digital platforms to tolerate harmful contents whenever disseminating them appears particularly profitable. The possible plurality of offended parties appears evident, just as the protected interests involve the public as well as the private dimension.[25]

This provision rather than constituting a tort, takes on a predominantly descriptive meaning. Coming from soft law, and not being mandatory, it is not assisted by any sanction. The breadth and potential vagueness of the protected interests could also raise concerns. Even if not contemplated as a binding rule, the aforementioned code of conduct on disinformation has been voluntarily accepted by Big Tech, so it can at least be attributed a value of moral suasion if not of standards of conduct, based precisely on the authority of the actors involved. But the question remains how this type of provision can be integrated into a more articulated policy to tackle online disinformation and whether Courts can enhance it without compromising the rule of law.[26]

3. Algorithm-amplified disinformation and systemic risk.

If the users of the traditional mass media were essentially passive recipients of information involved in a one-to-many relationship, in the digital platforms' era we are witnessing a change of paradigm.[27] The circulation of information is

[24] In the Italian case law, see C. App. sez. III Turin, Sent. June 22, 2021, n. 727 (The inauthentic phone call reproduced in a video does not constitute fake news with a defamatory and offensive scope of the Egyptian Museum, but falls within the right to political criticism, as it serves to argue with a promotional campaign, the contents of which are faithfully described), https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/03/Corte-dappello-Torino.pdf.

[25] See V Zeno-Zencovich, 'La disciplina della comunicazione in base al suo contenuto. Una proposta di inquadramento sistematico' (2020) 3 Dir inf 520-551; G Delannoi, 'De l'utilité de la notion de post-vérité', (2017) 197 Le débat, 4-12. For a renewed trust in the free marketplace of ideas, C Melzi D'Eril and G E Vigevani, 'Ma il mercato delle idee è proprio al capolinea? Considerazioni sparse a partire dal volume "il mercato delle verità" di Antonio Nicita (Recensione a Antonio Nicita, "Il mercato delle verità", Bologna, Il Mulino, 2021, pp. 240)', (2021) 3 MediaLaws, 279. Regarding the need for specific measures to combat online disinformation, see the most critical opinions of Vladimiro Giacché and Benedetto Ponti, while, in the opposite sense, Antonio Nicita, in the conference above: *La disinformazione: tra vecchi e nuovi media*, 24 maggio 2019, https://asimmetrie.org/eventi/la-disinformazione-tra-vecchi-e-nuovi-media/. See also B Ponti, 'La libertà di informazione al tempo della pandemia. Rilievi critici in margine all'istituzione dell'«unità di monitoraggio per il contrasto della diffusione di fake news relative al CoViD-19 sul web e sui social network»' (2020) 1 BioLaw Journal – Rivista di BioDiritto 636.

[26] About the legal relevance of the 'soft law', with particular reference to codes of conduct, G Teubner, 'Self-Constitutionalizing TNCs? On the Linkage of "Private" and "Public" Corporate Codes of Conduct', 18 Indiana Journal of Global Legal Studies (2011) 617; T E Frosini, 'Introduzione', in Id. (ed.), *La* Rule of Law *come costituzionalismo* (Bologna: Il Mulino, 2023) 14.

[27] About the concerns raised by the potentially global scale and the unprecedented velocity of the dissemination of false and extreme content, O Pollicino and G Pitruzzella, *Disinformation and hate speech*

here driven by a new business model: the hosting service is offered to users, in exchange for the raw material, i.e. the data and preferences that allow profiling for advertising purposes. [28] This exchange is carried out with constant interaction which could become surveillance and control over people.

Systemic risks are those phenomena, such as disinformation and electoral manipulation, discrimination against minorities and prejudice against minors online, which present a harmful potential amplified by the size of the platform (number of users in the European Union) and by the presence of systems or other elements that can significantly contribute to it, including all relevant algorithmic systems and their recommendation and advertising systems, with particular reference to the related data collection and use practices.[29] Thus the occasional risk of defamation, which was hidden behind the journalistic news, has given way to much more complex phenomena that are currently being studied and have yet to be fully understood. In particular, it has been observed that algorithms, through an analysis of the interactions that the user has had with VLOP or very large online search engines (VLOSE), present him with information that reflects and refers (echo-chambers) to the tastes, preferences

(Bocconi University Press, 2020); for a look at the civil liability of traditional media, see V Zeno-Zencovich and V Ricciuto, *Il danno da mass media*, (Cedam, 1990); C Verardi, 'Trasmissione di notizie inesatte e nesso di causalità del danno', case note to *Trib. Roma,* 22 June 1982, (1983) I Giust. civ. 636.

[28] See S Sica, G Giannone, 'I social network sites e il "labirinto" delle responsabilità', (2012) 12 Giur Merito, 2714; M Brenncke, 'A Theory of Exploitation for Consumer Law: Online Choice Architectures, Dark Patterns, and Autonomy Violations' (2024) 47 Journ Cons Policy 127-164.

[29] The categories of systemic risks identified are essentially: risks associated with the dissemination of illegal content, such as the dissemination of child sexual abuse material or illegal forms of hate speech or other types of abuse of their services to commit criminal offences, and the carrying out of illegal activities, such as the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products and illegally traded animals (Recital n. 80); the actual or foreseeable effects of the service on the exercise of the fundamental rights protected by the Charter, including but not limited to human dignity, freedom of expression and information, including media freedom and pluralism, the right to privacy, data protection, the right to non-discrimination, the rights of the child and consumer protection (Recital n. 81); the real or foreseeable negative effects on democratic processes, civic debate and electoral processes, as well as on public security (Recital n. 82); similar concerns related to the design, operation or use, including by manipulation, of very large online platforms and very large online search engines, with actual or foreseeable negative impacts on the protection of public health and children and serious negative consequences for the physical and mental well-being of the person or for gender-based violence. Such risks may also arise from coordinated public health disinformation campaigns or from the design of online interfaces that may stimulate the behavioral addictions of service recipients (Recital n. 83). As highlighted by Recital n. 79: "In determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess whether the potential negative impact can affect a large number of persons, its potential irreversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact.". See also Recital n. 84, DSA: "When assessing such systemic risks, providers (…) should focus on the systems or other elements that may contribute to the risks, including all the algorithmic systems that may be relevant, in particular their recommender systems and advertising systems, paying attention to the related data collection and use practices. They should also assess whether their terms and conditions and the enforcement thereof are appropriate, as well as their content moderation processes, technical tools and allocated resources. When assessing the systemic risks identified in this Regulation, those providers should also focus on the information which is not illegal, but contributes to the systemic risks identified in this Regulation. Such providers should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation. Where the algorithmic amplification of information contributes to the systemic risks, those providers should duly reflect this in their risk assessments.". Recently, it has been acutely highlighted by the jurisprudence that: "The reasons behind the increase in hatred, even in the absence of differences in content between online and offline hate speech, have been identified in some structural components of the network, which are considered to act as facilitating factors of discriminatory messages, consequently increasing their harmful potential (....)" (*Tribunale di Roma. Sent. n.* 17909/2022, n 22).

and beliefs of the user himself (cherry picking and confirmation biases). Regardless of the truthfulness and reliability of the contents, they suggest those that are most capable of stimulating attention and reactions. Thus, a psychological mechanism called "intermittent positive reinforcement" is produced, which stimulates the release of dopamine, a neurotransmitter hormone that causes comfort and euphoria.[30] These techniques had already been experimented in slot machines, then transposed into computer games and, finally, adapted to the websites design. [31] This, in order to induce a strong need to be connected with that medium, favors a progressive social isolation (filter bubble) and, in the most serious cases, the onset of a real addiction.[32] It was emphasized that the mechanism tends to produce a polarization of opinions, with the consequent formation of conflicting factions. At the same time, this is highly desirable by providers as it generates an exponential growth in communications and attention to online content, resulting in increased advertising revenue.[33]

Due to the aforementioned experience of VLOP, two levels of analysis of online disinformation can be distinguished. If fundamentally the wrongful acts are based only on the analysis of the single content disseminated, today there are further detrimental effects caused by the peculiarities of the medium used. [34] In the latter case we have a specific element, compared to simple dissemination, as it is the method of conveying content that is, first of all, under

[30] Cfr. V R Bhargava and M Velasquez, 'Ethics of the Attention Economy: The Problem of Social Media Addiction', (July 2021) 31:3 *Business Ethics Quarterly*, 327 and the specialist bibliography cited therein; D T Courtwright, *The Age of Addiction: How Bad Habits Became Big Business* (Harvard University Press, 2019). For confirmation of the deleterious effects of the social network Instagram on minors, see the impressive report of the experiments conducted by the same company: G Wells *et al.*, 'Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show. Its own in-depth research shows a significant mental-health issue that Facebook play down in public' (*The Wall Street Journal*, *Sept.* 14, 2021). About the case of Tiktok, see T D Hobbs *et al.*, ''The Corpse Bride Diet': How TikTok Inundates Teens With Eating-Disorder Videos. The app's algorithm can send users down rabbit holes of narrow interest, resulting in potentially dangerous content such as emaciated images, purging techniques, hazardous diets and body shaming' (*The Wall Street Journal, Dec.* 17, 2021).

[31] See D Spohr, 'Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media', (2017) 34 Bus Info Rev 150, 151; A Gordon-Tapiero and Y Kaplan, 'Unjust Enrichment by Algorithm', (2024) 92 Geo Wash L Rev 305-358. See also Recital n. 69 (DSA): "When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups. Online platforms are particularly sensitive environments for such practices and they present a higher societal risk".

[32]Scientific evidences in Bhargava, Velasquez, 'Ethics of the Attention Economy' (n 31), 321-322; Ursula Oberst *et al.*, 'Negative consequences from heavy social networking adolescents: The mediating role of fear of missing out', (2017) 55 Journal of Adolescence 51-60; N A Farahani, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023). On rhetorical devices of online disinformation campaigns, Carlos Diaz Ruiz *et al.*, *Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies*, 42 (1) *Journal of Public Policy & Marketing,* 18-35 (2023) and 20-24 on identity driven controversy and anti-scientific reasoning supported by an alignment with previous traditions (such as the biblical tradition). See also Vladimiro Giacché, *La fabbrica del falso. Strategie della menzogna nella politica contemporanea* (DeriveApprodi, 2011).

[33] Cf. E Pariser, *The Filter Bubble. What the Internet Is Hiding from You*, 16 (Viking 2011); C R Sunstein, *#Republic: Divided democracy in the age of social media* (NJ: Princeton University 2017); L M Kahn, 'The Separation of Platforms and Commerce' (2019) 119 Colum L Rev 973, 987.

[34] About the radical changes induced by paradigm shift in communication technologies, M McLuan, *Understanding media. The Extension of Man*, (Mc Graw-Hill Book Company 1964).

discussion, and which enhances the cognitive distortion effects that the disseminated content would have in itself.

4. Cooperation duties and the role of the EU Commission.

The DSA deals extensively with disinformation, which it considers an important emergency. The regulation does not seem to opt for the creation of an ad hoc tort, and the doubt remains that it is a phenomenon with uncertain contours, capable of remaining in limbo. In fact, knowledge or awareness of the illegality of the content is not always required.[35] In short, the DSA does not introduce a broad concept of disinformation that is illegal in itself: the obligations of the platforms concern only the reporting of manifest and specific violations. Nonetheless, certain harmful developments of the fake news are amplified by the same operating mechanisms of digital platforms, based on artificial intelligence and user profiling. Although online disinformation is not unlawful in itself, it can amount to a systemic risk, and attention is drawn to the need to contain its possible pathological and dangerous developments. In this regard, providers are required to adopt a series of preventive measures, under threat of penalties and other corrective sanctions in the event of non-compliance.

It ranges from active dissemination measures[36] to forms of blocking and demonetization of accounts, but also the targeted use of artificial intelligence in the positioning of information within search engines.[37] In this sense, in addition to the labelling obligations regarding AI-generated content, imposed on large platforms by the Artificial Intelligence Regulation, the duties of transparency and disclosure become as relevant as the outputs of AI systems are artificially generated or manipulated.[38]

It can be underlined that, in addition to focusing on command and control, here entrusted mainly to the European Commission, the deregulation method is increasingly followed. That is, the aim is to obtain compliance from the operators themselves, who are asked to adopt codes of conduct and action

[35] Cf. Recital n. 53 and art. 6 (Hosting).

[36] For example, by providing that "where a provider of an online platform allowing consumers to conclude distance contracts with traders becomes aware, irrespective of the means used, that an illegal product or service has been offered by a trader to consumers located in the Union through its services, that provider shall inform, insofar as it has their contact details, consumers who purchased the illegal product or service through its services of the following: (a) the fact that the product or service is illegal; (b) the identity of the trader; and (c) any relevant means of redress." (art. 32, Right to information).

[37] See L McIntyre, *On disinformation. How to fight for truth and protect democracy* (MIT Press 2023); K Kertysova, 'Artificial intelligence and disinformation. How AI changes the way disinformation is produced, disseminated, and can be countered' (2018) 29(1-4) Security and Human Rights 55-81; N Bontridder and Y Poullet, 'The role of artificial intelligence in disinformation' (2021) Jan 3 Data & Policy 32.

[38] Cf. Recital n. 136, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Cf. C Marsden and T Meyer, *Regulating disinformation with artificial intelligence: effects of disinformation initiatives on freedom of expression and media pluralism* (Brussels: European Parliament 2019). The issue of labeling invests, for example, the dangerous phenomenon of deep fakes: fake images and videos artfully passed off as originals, but born from AI, which, in some cases, can produce very harmful deceptive and confusing effects. See also M Cazzaniga, 'Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai "deepfakes"' (2023) 1 MediaLaws 170-187; M Mezzanotte, '"Fake news", "deepfake" e sovranità digitale nei periodi bellici' (2022) 33 *federalismi.it* 44-65.

plans that prevent such risks. As already happened with regard to personal data in the GDPR, also the systemic risks related to disinformation can be treated in terms of regulation by design.[39] In this sense, it can be underlined that the DSA provides that compliance with its rules must be guaranteed by VLOP through independent audits. [40] As stated by art. 72 (Monitoring actions) "The Commission may take the necessary actions to monitor the effective implementation and compliance with this Regulation by providers of the very large online platform and of the very large online search engines. The Commission may order large online platform to provide access to, and explanations relating to, its databases and algorithms. Such actions may include, imposing an obligation on the provider of the very large online platform or of the very large online search engine to retain all documents deemed to be necessary to assess the implementation of and compliance with the obligations under this Regulation".

Although a general obligation of preventive surveillance has not been introduced, providers will have to cooperate in a more structured and qualified way to prevent wrongful activities, by operating transparently, especially with regard to the algorithms used, collecting reports and intervening promptly. The requirements to equip themselves with internal procedures and algorithms adequate to address the so-called systemic risks (articles 34 et seq.) now deeply bind VLOP. [41]

According to the DSA, the EU Commission's power clearly prevails over the powers attributed to the authorities of the Member States on the subject of VLOP and VLOSE (Chapter IV, section 4) [42]. Precisely because of the complexity of the phenomenon, the activity of sanction constitutes only a part of a more complex system.

The first step consists in seeking information about possible violations, which allows to agree with the providers a series of corrective measures and intervention plans that will then be checked out in their actual implementation.

Unless there are specific precautionary needs, the application of prohibitory injunctions, such as the suspension of a social network, seems to represent only the last resort since it can only be ordered in court.

---

[39] Cf. P Hacker, 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law' (2023) 29 Eur Law Journ 170: "When algorithmic manipulation operates not through hidden influence, but (also) through the impairment of rational choice, withdrawal rights will likely not suffice. Vulnerable consumers may not necessarily exercise these rights, for various cognitive reasons (e.g. endowment effect; status quo bias; procrastination; or simple convenience). Hence, it seems worthwhile to discuss strategies for mitigating such influence ex ante, rather than attempting to correct distorted outcomes ex post via traditional UCPD enforcement or withdrawal rights. In this vein, an important strategy is what will here be termed 'non-manipulation by design'". See also Trib. Roma, Sent. n. 17909/2022 (n 22): "The DSA regulation provides for obligations proportionate to the size of the platform and a new culture of prevention of systemic risks, from disinformation to illegal content. The Regulation, which will come into force in 2023 and is therefore not applicable in the present case, confirms the path taken by the provider regarding the initiatives to also discourage the spread of hate speech, especially through the internet (as well as providing for a control more stringent public on the platforms)".

[40] See Recital n. 92 and art. 72 (Monitoring actions), par. 2 (DSA).

[41] It is worth noting the criticisms of those who consider the DSA's approach as potentially authoritarian, since it would give the EU Commission excessively broad discretionary powers, to the detriment of freedom of expression. See, for example, A Chander, 'When the Digital Services Act Goes Global' (2023) 38 (3) Berkeley Technology Law Review 1071, 1082, noting that "an authoritarian state could use the recommendation and guidelines powers to pressure platforms to implement rules to control speech".

[42] Articolo 51 (Powers of Digital Services Coordinators).

Penalties can reach up to 6% of the of the annual worldwide turnover of the provider of intermediary services concerned in the preceding financial year.[43] This centralization of powers on the Commission corresponds to the need for efficiency and cost-effectiveness of the control and sanction system, also in terms of the use of technological resources. Given the transnational dimensions of the providers, it would be better to join forces since it is cost-ineffective to multiply the proceedings in all the Member States. However the system designed by the DSA does not seem easy to implement, especially where it provides for coordination mechanisms between national authorities and the Commission (art. 66).

The active role of other social actors, in particular trusted flaggers and fact checkers, is considered strategic, but some aspects still need to be properly assessed[44]. Consider the problem of the priority to be given to reports from such accredited subjects[45].

On a practical level, the first interpretative role seems to be up to digital platforms. In fact, their terms of service usually provide private powers of moderation and removal of misleading or harmful contents (e.g. those contrary to overriding public interests). But, absent a specific legislative provision, such clauses could be considered void, in the light of the fundamental right to freedom of expression.[46]

---

[43] See art. 52(3), DSA.

[44] In this regard, a role in the study and promotion of regulatory initiatives is recognized to the European Digital Media Observatory (EDMO), an independent observatory that brings together fact checkers and academics operating in the field of online disinformation, social media platforms, journalists and other experts in the media sector.

[45] Think about the figure of 'trusted flaggers', introduced by art. 22 of the DSA which, for example, in Italy has found a complete regulation in Annex A to the AGCOM resolution no. 283/24/CONS, 'Procedure Regulation for the recognition of the qualification of trusted flaggers pursuant to art. 22 of the Digital Services Regulation'.

[46] See *Tribunale di Roma, Sentenza n. 17909* (n 22). The Italian Judge, dealing with the directive 2000/31/EC, stated that "Even if there is no general obligation of supervision - except that the latter could be the result of a free choice of the intermediary -, nevertheless art. 14 of the Directive imposes surveillance obligations on these intermediaries in specific cases with the result that, in certain cases, the host provider must prevent a breach and must contribute to avoiding new violations". And so on: "In the wake of these initiatives, the new European regulation on digital services, approved on 5 July 2022, with the declared aim of ensuring a safe and responsible online environment to protect users' fundamental rights. The regulation provides for obligations proportionate to the size of the platform and a new culture of prevention of systemic risks, from disinformation to illegal content. It will enter into force in 2023 and is therefore not applicable in the present case, but it confirms the path taken by Facebook with regard to initiatives to also discourage the spread of hate speech, especially through the network (as well as providing for more stringent public control over platforms)". In the same sense, Trib. Varese, Ord. sec. I. civ., 2 August 2022, no. 1181 (Facebook's general terms and conditions of contract - so-called community standards -, which already provided for the prohibition of "disinformation and unverifiable rumors that contribute to the risk of violence or imminent physical harm", had been updated to also counter disinformation related to the pandemic, providing for the protection of public health as a limit to freedom of expression. Therefore, the removal of posts and suspension of accounts by Facebook are not illegal if they are aimed at countering misinformation harmful to public health, with particular reference to content tending to discredit the safety of the vaccination campaign and to spread unjustified alarms). For a critical view on the binding effect of standard terms, see G Alpa, 'On Contractual Power of Digital Platforms' (2023) 34 (3) EBLR 377-390. On this point, see the very recent *Trib. Rome (sec. XVII civ), Sent. no. 9653* of 5 June 2024 (unofficial copy of the Judgment available at the permalink https://apps.dirittopratico.it/sentenza/tribunale/roma/2024/9653.html#829cc) which condemned Google to reactivate monetization and to compensate the broadcaster Radio Radio (200,000 euros, equal to 5,000 euros per month) for the damage resulting from the deactivation of the monetization service on YouTube (which allowed the well-known broadcaster to benefit from paid ads). This deactivation had been ordered by Google, alleging that some "misinformative" videos in the Covid-19 health sector were uploaded to that channel "not compliant with the policies of the platform's Partner Program - and,

Theoretically, social networks themselves could spontaneously correct their algorithms, privileging quality information and mitigating the mechanism of personalization. [47] But it is certainly more likely that they will neglect to do so, if this conflicts with their economic interests. [48] So civil deterrence could be useful in encouraging such a task. But there could be many doubts about how to concretely achieve it.
For example, take the anti-evolutionism and denialist theories of climate change with respect to which the following question could be asked: if scientific evidence must necessarily guide judicial decisions, to the detriment of other beliefs and convictions, why should such reasoning not apply in the marketplace of ideas, when they serve to influence movements of opinion and political majorities? [49] Although the environmental issue does not appear among the systemic risks considered in the DSA, it is included in the public goods enshrined in the Code of Conduct on Disinformation that has been voluntarily accepted by the main platforms. Would this be enough to make climate change denial theses illegal? What remedy should be adopted, if any? Perhaps removal or blocking could appear excessively sharp and, at least in certain cases, it would be sufficient to accompany those messages with warnings that recommend turning to more reliable sources, available with a specific link. Of course, this ability to analyze and act *cum grano salis* has a cost, which the platforms should be able to absorb more easily given their better and more solid position.[50]

therefore, contrary to the contractual provisions - which would have allowed the manager of the social network to exercise the right to unilaterally deactivate the monetization function". However, the judge considered such behavior unlawful, and compensable for the related damage, reasoning: "it is quite clear that these rules were introduced after the conclusion of the contract between the parties, i.e. after the occurrence of the well-known epidemic, so that the negotiating consent of the contracting parties cannot have been formed on them. That consent was instead essential so that the contractual provisions could be effective and have the force of law between the parties (art. 1372 of the Italian Civil Code)". Skeptical towards a new digital information ecosystem based on ad hoc rules and more optimistic towards the civil law system based on the judicial control over the fairness of the terms of service, U Ruffolo, 'Piattaforme e "content moderation" negoziale' (2024) 2 Giur it 442-452.

[47] Recital 88 of the DSA provides for the following: "Providers of very large online platforms and of very large online search engines may need to reinforce their internal processes or supervision of any of their activities, in particular as regards the detection of systemic risks, and conduct more frequent or targeted risk assessments related to new functionalities. In particular, where risks are shared across different online platforms or online search engines, they should cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures. They should also consider awareness-raising actions, in particular where risks relate to disinformation campaigns.".

[48] See D M J Lazer *et al.*, 'The Science of Fake News. Addressing fake news requires a multidisciplinary effort' (2018) 359 (6380) 1094-1096.

[49] See B Leiter, 'The Case Against Free Speech', (2016) 38 Sidney Law Review 407, 415.

[50] Some recall the famous theory of the 'cheapest cost avoider', by G Calabresi, *The Cost of Accidents: A Legal and Economic Analysis* (Yale University Press 1970) and hope that, also thanks to deterrence, a proactive function of social media on issues of pressing public interest can be strengthened. See K Tokeley, 'The Power of the "Internet of Things" to Mislead and Manipulate Consumers: A Regulatory Challenge', (2021) 2 Notre Dame J on Emerging Tech 135: "The advertiser and the AI creator are also in a better position than the consumer to both bear the loss caused by the misinformation (by spreading the costs via price adjustments) and prevent misinformation (by abandoning a black box AI system if it is too unpredictable)".

5. Civil liability of digital platforms.

The DSA does not deal with disinformation by directly prohibiting certain harmful illegal content (false, misleading, deceptive etc.). This aspect is, in fact, already addressed by various provisions in each Member State, which also reflects the different value choices of each one. According to the DSA, the focus is rather on operational obligations aimed at mitigating systemic risk. This essentially concerns the failure to prevent a wide circulation of that dangerous content, precisely by omitting preventive measures, or subsequent measures required by the administrative or judicial authority. Such systemic disinformation could affect both public and private interests. In the latter case, compensation would play an important role. The basis for this type of damage does not refer to the 'notice and take down' mechanism, but is instead based on the failure to mitigate the risk. In other words, it is the negligence of the providers for not having adapted the design and algorithms that govern the functioning of the platform and the organization of its contents.

As the DSA shows, effective public command and control does not preclude but rather helps to protect collective interests, with particular reference to groups homogeneously affected by the violation of the law. There is a close relationship, and a mutual feeding, of the two phenomena, fake news and hate speech and the case history is multifaceted. [51] In the events of Capitol Hill, the false accusations of electoral fraud formulated by Trump, and amplified by Facebook algorithms, have fomented the assault on Congress by groups of his followers. This has led to the hypothesis of the remedy of class actions for unjust enrichment, aimed at obtaining the reversion of profits (disgorgement of profits) unduly obtained by the platforms.[52] The profits obtained through manipulative information and unlawful processing of personal data may seem negligible, if considered individually, but would reach considerable sums, aggregating millions of user data. [53]

---

[51] The cases are different. Just think of the dissemination of prejudices against ethnic minorities, or scientifically unfounded news that harms the dignity and safety of certain entities or people.

[52] For an analysis of the U.S. litigation which focuses on the active dissemination of content based on discrimination, disinformation, extremism and polarization and democratic erosion, see Gordon-Tapiero and Kaplan, *Unjust Enrichment by Algorithm* (n 32) 328-329; V Ndior, 'Les réseaux sociaux et l'administration Trump' (2022) 184 *Hérodote* 201-215; Y Benkler *et al.*, 'Mail-In Voter Fraud: Anatomy of a Disinformation Campaign' (2020) 6 Berkman Center Research Publication 1-49. On the consequences of the vulnerability induced by robots and apps in consumers, W Hartzog, 'Unfair and deceptive robots' (2015) 74 Maryland Law Rev 785-788. The original perspective of the waste of time suffered by the unsuspecting user, subject to algorithmic information manipulations, refers to the difficult, and necessarily equitable, judicial evaluation, probably to be resolved on the level of collective deterrence. Cf. L T Visscher, 'Time is Money? A Law and Economics Approach to 'Loss of Time' as Non-Pecuniary Loss' (2014) 5 (1) Journal of European Tort Law, 35-66. An action for damages can also be envisaged in which the damage would be identified in the undue exploitation of the consumer's vulnerability, thanks to the use of systems that take advantage of consumer biases. Cf. Brenncke, 'A Theory of Exploitation' (n 29) 131 ss.

[53] Cf. Gordon-Tapiero, Kaplan, *Unjust Enrichment by Algorithm*, (id.) 351 ("(…) when distribution of class action awards to individual users is impracticable or inappropriate, courts can use cy pres relief as an alternative to traditional class action remedies. Under this doctrine, courts can have the class defendant donate part of the award to a charitable cause related to the substance of the lawsuit. In the context of platform personalization, such charitable causes might include digital literacy and online safety among vulnerable groups. Another venue for recovery would be for courts to order uid class recovery. Under this doctrinal alternative, courts can obligate the platform to award users with goods, services, future price reductions, or other monetary equivalents as a substitute to a monetary award."), citations omitted. On the

It is worth noting that art. 54 (Compensation) of the DSA states that recipients of the service have the right to request compensation, in accordance with Union and national law, from intermediary service providers for damages or losses suffered as a result of a violation of the obligations established by this Regulation. Despite a generally little role of private remedies compared to public enforcement, in the EU approach to disinformation risk, this provision is important. If read together with the further indication of Recital no. 121,[54] it means that, in terms of compensatory remedy, all pre-existing options remain open, for example, those of pecuniary and non-pecuniary damages (e.g. art. 2043 and 2059 Italian Civil Code).

A potential convergence of protections regarding personal data and the commercial/consumer aspect, that is "unfair commercial practices", should not be underestimated. If we observe the phenomenon of disinformation intended, through algorithms, to influence minors or psychologically more exposed subjects, this could be traced back to aggressive commercial practices. There is no doubt that some groups of people can become targets more than others, precisely thanks to common characteristics that the algorithm itself detects and that this leads to homogeneous prejudicial effects. They concern both the economic choices made and the non-pecuniary losses suffered by the manipulated users.[55] However, proving collective damages in this type of circumstances can be more complex than simply reporting individual harmful contents, which are detectable *ictu oculi*. In addition to external fact checking, the evidence of unlawful practices may come from within the provider's company, as is the case with the exhibition of documents, testimonies of former employees, anonymous reports and whistleblowers. EU policies have developed important tools to raise alarms and provide useful details to report violations perpetuated by large digital platforms and search engines under the DSA.[56] Moreover, it should be underlined that the quantification of compensation can be linked, in addition to the damage suffered, to the seriousness and nature of the unfair commercial practice, and to other relevant circumstances, with a view to deterrence.[57]

Since dealing with large platforms, in terms of algorithms intelligibility, requires large investments and very specific technical skills, this goal can be better achieved through public enforcement.[58] Nevertheless, there is also

---

intertwining of economic and moral interests in the all-encompassing relationship between users and platforms, see P Hacker, 'Manipulation by algorithms' (n 40) 142-175; N Helberger *et al.*, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 Journ Cons Policy 175-200.

[54] "(…) a provider of intermediary services should be liable for the damages suffered by recipients of the service that are caused by an infringement of the obligations set out in this Regulation by that provider. Such compensation should be in accordance with the rules and procedures set out in the applicable national law and without prejudice to other possibilities for redress available under consumer protection rules.".

[55] See *supra* note 52.

[56] See, for example, the recent DSA whistleblower tool, launched by the Commission (Press release, 30 April 2024, Directorate General for Competition. Directorate General for Communications Networks, Content and Technology: Commission launches Whistleblower Tools for Digital Services Act and Digital Markets Act).

[57] See, for example, art. 27, par. 15-*bis*, Consumer code (Italy).

[58] The Commission has already undertaken investigations to verify the compliance of large platforms with the DSA rules. On October 2, 2024, a control initiative was announced against TikTok, YouTube and Snapchat aimed at understanding the way in which videos and information are suggested to users, as well as the prevention measures taken by the aforementioned platforms in order to spread harmful content. See *EU requests info from YouTube, Snapchat, TikTok on content algorithms,* Reuters, October 2, 2024. In particular,

room, at the state level, for compensatory actions, both individual and collective.

In order to address collective harm resulting from unfair commercial practices, reference should be made to the EU Directive 2020/1828 on representative actions[59] recently transposed into national law (e.g. art. 27, paragraph 15-bis, and arts. 140-ter to 140-quaterdecies, Italian Consumer Code).[60] The latter, although still far from the more efficient and rapid US class action model, allow, among other things, to bring the case before the national jurisdiction, without having to wait for the response of the EU Commission. Although the DSA seems to prefer gradual solutions, like the enhancement of co-regulation with large digital platforms which is akin to self-regulation, it leaves open the possibility that violations of cooperation duties may give rise to damages referable to the collective interests of consumers. It lies within the competence of Member States to deal with such tortious liability of digital platforms for failing to deal with systemic risk. Examining EU soft law, we have seen that a "catch-all provision" significantly focuses on the malicious spread

---

the hypothesis is that people considered vulnerable are offered fake news related to political issues, or content that promotes behaviors that can generate eating disorders, or lead to depression or drug abuse. Platforms should, therefore, be induced to introduce corrective measures, such as allowing users to hide certain types of contents. Another investigation was launched in May 2024, against Meta, the parent company of Facebook and Instagram, to verify whether the algorithms had been set up in such a way as to induce addictions in children, exploiting their ingenuity and lack of experience. With regard to the proceedings previously launched against the social network X, on 12 July 2024, the Commission notified the preliminary findings, which show some violations of the DSA, in particular of Articles 25 (Online interface design and organisation), 39 (Additional online advertising transparency) and 40(12) on freedom of information and accessibility of data: "Providers of very large online platforms or of very large online search engines shall give access without undue delay to data, including, where technically possible, to real-time data, provided that the data is publicly accessible in their online interface by researchers (…)". First of all, the investigation ascertained the use of the Blue Checkmark system which compromises the authenticity and integrity of accounts, furthermore it detected specific characteristics (design features) of the algorithms which prevent the detection of risks inherent to online advertising, also because their archiving and traceability are omitted. Finally, in contravention of the DSA, X impedes independent access to public data for researchers by imposing high fees and dissuasive procedures for access. These conclusions were reached through a detailed investigation, which included: review of internal company documents, expert advice, and collaboration with national authorities. If these preliminary findings are confirmed, the Commission could impose fines of up to 6% of annual turnover and order corrective measures. Failure to comply with the latter can lead to enhanced enforcement, as well as further penalties to induce compliance. Cf. *Commission sends preliminary findings to X for breach of the Digital Services Act, Press Release 12 July 2024*. In recent times, in addition to the moratorium imposed on the TikTok platform by January 2025, there has been news of the intensification of lawsuits against it, both at the federal and state level, for unfair and deceptive practices and violation of the privacy of child consumers: the social network would be designed to induce addiction through the scrolling mechanism with harmful effects both psychological, as physical. On the platform's side, defensive arguments are exposed such as the many initiatives put in place to mitigate these risks and the danger to the freedom of expression of content creators. See S Maheshwari and D McCabe, 'TikTok Faces Barrage of Lawsuits Around Teens and Mental Health. More than a dozen states sued TikTok on Tuesday for creating an app designed to be addictive to children and teenagers' (The New York Times October 8 2024).

[59] As implied by art. 2 (1), the Directive applies to representative actions brought against such infringements referred to in Annex I (14), including such provisions as transposed into national law, that harm or may harm the collective interests of consumers.

[60] About class actions in the European Union, see D Fairgrieve and R Salim, 'Collective Redress in Europe: Moving Forward or Treading Water?' (2022) 71(2) International and Comparative Law Quarterly 465-479; for a look at tortious liability in EU private law, see G Alpa and M Andenas, *European Private Law* (Pacini editore 2022, 283-285). On representative actions and online damages, see X Kramer and E Silva de Freitas, 'International tech litigation reaches the next level: collective actions against TikTok and Google' (Conflict of laws. Net. Views and News in Private International Law, March 12, 2024) and Id., 'Who can bite the Apple? The CJEU can shape the future of online damages and collective actions' (id. Jan. 18, 2024).

of harmful disinformation for profit purposes. And yet that “catch-all provision”, even if not binding, could be a useful key to understanding the materialization of a public harm especially when there is a persistent breach of duty to cooperate.