FERMI
FAKE NEWS
RISK MITIGATOR

NAVIGATING DISINFORMATION: A COMPREHENSIVE GUIDE

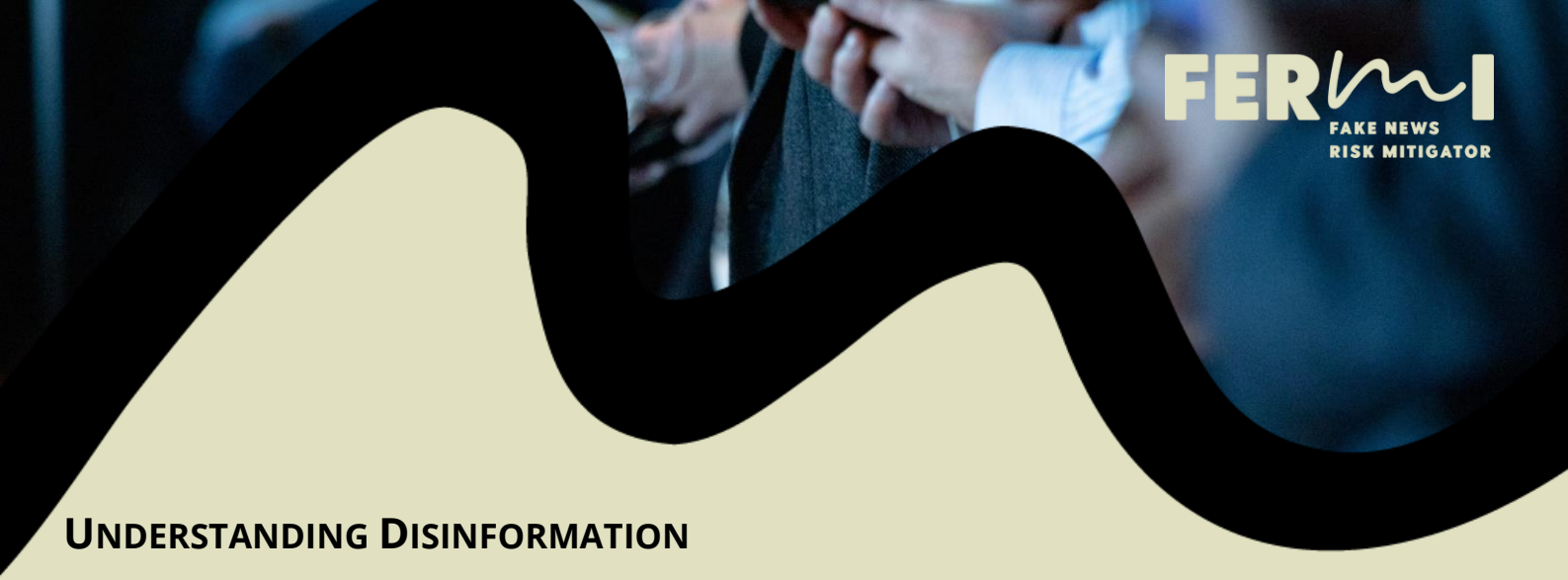
This guidebook has been designed in the context of FERMI (Fake nEws Risk MItigator) [Project 101073980], a Horizon Europe project that studies and attempts to counter the root causes, spread and implications of disinformation and fake news. This guidebook is inspired and derived primarily from the insights shared during the FERMI webinar "A dive into the societal landscape of disinformation - Balancing between Law Enforcement and Fundamental Rights to Increase Digital Trust" which took place on 23/02/2024.

The aim is to equip the reader with some basic knowledge and resources to navigate the murky waters of disinformation. This guidebook should ideally be read before or after viewing the webinar recording (found on the FERMI website) thus offering a comprehensive package that provides in-depth knowledge, fosters understanding, and encourages critical engagement with the topic of disinformation.

PARTNERS

Funded by the European Union

fighting-fake-news.eu



Understanding Disinformation

Disinformation is a complex phenomenon, its complexity lies not only in challenges to properly define it but also in the way it manifests and impacts the social fabrics of any society. Disinformation is not a new phenomenon, however the digital technology involved in online disinformation has recently arisen and this has contributed to exponentially increasing the impact that disinformation has. From the propaganda techniques to the algorithm-driven amplification of false narratives on social media platforms, the strategies and reach of disinformation campaigns have been significantly evolving. In the digital society we live in, the intricate web of disinformation, misinformation, and malinformation further complicates the landscape of accessible information. Emphasis should be placed on the intention behind the spread of false information since this can be the differentiating factor.

There are subtle distinctions among these concepts, focusing on the intent behind the spread. Misinformation, unlike disinformation, is spread without a malicious intent, often stemming from misunderstanding or miscommunication. Malinformation, on the other hand, involves the dissemination of truthful information with the intent to harm. Understanding these distinctions and the respective challenges in defining and tracing disinformation is key to developing effective strategies to mitigate their impact and guide the efforts of individuals, organisations, and governments in safeguarding the integrity of information.

The Legal Landscape of Disinformation

Defining disinformation within the European Union and beyond is burdened with challenges. Despite several policy documents and attempts at creating a common understanding, there is no universal agreement on what constitutes disinformation.

What has been produced are a number of policy documents, in one of these key documents we can find a commonly used definition of disinformation which is being used in the policy making environment. Therein, “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” [1]. This lack of consensus not only complicates legal and regulatory efforts but can also impede international cooperation in combating its spread.
By briefly analysing this commonly used definition of disinformation one can see the nuances of disinformation and the difficulties in tracing it and distinguishing it from other forms of false or misleading content.

[1] European Commission, *Action Plan against Disinformation* (Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018),p. 1. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0036

Challenges in legally defining Disinformation

Disinformation, unlike other types of illegal or harmful content, is more likely to be confused with legal content so there is risk of spill-over effect. Furthermore, the intention to gain economic profit or deceive the public is challenging to evaluate and a distinction must be made between malicious disinformation actors and individuals who accidentally share false information. In addition, because in most of the cases these actions/intentions cannot be traced back to one single actor, but to a multitude of actors.

The actions of assessing the potential for causing public harm in advance, such as negatively affecting democratic processes, is really challenging. Identifying what is false (or misleading) requires a careful assessment of context and circumstances (this can be particularly challenging online).

Additionally, determining the falseness or misleading nature of information demands a meticulous evaluation of the context and circumstances, a task that becomes especially difficult in the online environment. These complexities and the lack of consensus, in defining the phenomenon poses substantial difficulties in appointing standardised legal measures to battle/tackle disinformation. In combating disinformation, the protection of fundamental rights and democratic values should be at the core of these efforts.

Article 51.1 of the EU Charter of Fundamental Rights mandates that any restrictions on rights and freedoms recognised by the Charter must be legally established, essential, and proportionate, respecting the core of those rights. Such limitations are permissible only if they are necessary to achieve objectives of general interest recognised by the EU or to safeguard the rights and freedoms of others. According to the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) case law, laws imposing restrictions must be accessible, clear, and non-discriminatory, ensuring that any limitation on fundamental rights is predictable and justified by a legitimate public interest, such as national security or crime prevention.

EU Policies on Disinformation

The European Union has recognised the threat posed by disinformation, leading to the development of several strategies to counter it. Notable initiatives include the “European Action Plan against Disinformation”, which aims to enhance the EU's capability to identify and counteract disinformation, encourage cooperation and joint responses, while also mobilise the private sector to fulfil commitments against disinformation, and improve societal resilience. “The Code of Practice on Disinformation”, has a more targeted approach, it enlists tech companies in efforts to reduce the spread of disinformation. It is specifically aimed at online platforms and the advertising industry. This can be viewed as a self-regulatory framework, with commitments to fight disinformation through various measures such as increasing transparency, promoting trustworthy content, and empowering users.

Risks in Regulating Disinformation – Impact on Fundamental Rights

Crafting legislation that effectively counters disinformation without infringing on freedoms poses significant challenges. Legal debates within the EU often centre on identifying the threshold where regulatory measures become necessary to protect public interests without overstepping into censorship or violating rights.

Disinformation can be considered a form of expression, albeit potentially harmful. The need to regulate disinformation, intersects with fundamental freedoms and privacy concerns. Restricting disinformation under the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (EUCFR) requires a delicate balance to avoid invading on the right to freedom of expression, only permissible for legitimate public interests. However, these attempts bear significant risks, including the potential for broad or vague definitions that unduly restrict lawful speech, leading to a chilling effect where individuals self-censor out of fear of sanctions. Furthermore, law enforcement agencies' efforts to detect disinformation actors for crime prevention or investigation can impact privacy and data protection rights. The EU strongly protects these rights under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive, raising concerns about mass surveillance and disproportionate data access and retention. This surveillance risk, particularly when involving sensitive information like political opinions or religious beliefs, further compounds the chilling effect on freedom of expression, underscoring the complex interplay between safeguarding public interests and protecting individual rights.

Balancing Act: Navigating Disinformation Mitigation and Fundamental Rights

While EU law does not regulate disinformation directly, the Digital Services Act (DSA) aims to mitigate it through collaboration between online platforms, search engines, and public authorities. Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs) are mandated to assess systemic risks, especially those affecting civic discourse and public security, and implement necessary risk mitigation measures. This includes prioritising responses to "trusted flaggers," who may be LEAs. However, there are challenges such as, as aforementioned, the lack of a uniform EU definition of disinformation, leaving VLOPs and VLOSEs with considerable discretion in adopting mitigation measures and employing automated moderation tools. This in turn raises concerns about fundamental rights, including the necessity and proportionality of measures that might limit these rights. The regulation of content moderation between public and private entities must ensure respect for fundamental rights, incorporating transparency and fairness in takedown measures. Additionally, what is essential is to establish an independent oversight mechanism to balance the cooperation on content moderation and safeguard against the infringement of fundamental rights.

Law enforcement agencies should approach disinformation within the bounds of the law, while upholding fundamental rights and democratic values. Enhanced protection of sensitive personal data is a crucial step given the intrusive potential of surveillance technologies. Any measure to combat disinformation must be clear and predictable to prevent overreach, with an established, albeit indirect, link to the legitimate objectives they aim to fulfil, ensuring proportionality relative to the severity of the threat

The Broader Societal Impact of Disinformation

As analysed above, one of the main challenges we face with the phenomenon of disinformation starts from the outset, i.e., establishing a uniform definition of disinformation. This difficulty in defining disinformation stems from the various methods through which information can be distorted to misinform, beyond the content itself. Thus, a more nuanced understanding of disinformation is required. Disinformation is a formidable force which is contributing to what is increasingly known as 'information disorder'. Information disorder encompasses a range of complications related to how information is created, shared, and received particularly in the digital age. It is characterised by the spread of misinformation, disinformation, and malinformation.

Information disorder is not just a technical issue but also a societal issue which involves the exploitation of emotional and psychological vulnerabilities. The essence of disinformation lies in the intent to weaken the information space by various means, not limited to the spread of false content but also through the things left unreported. Disinformation's negative impact on society is not necessarily the content or the lie itself but the ability to spread and become embedded in public discourse.

Disinformation’s reach extends into the realm of journalism, where media manipulation and editorial omissions can shape narratives and, consequently, public opinion. The impact of disinformation is profound because is not restricted to the immediate impact of false narratives but includes the long-term erosion of societal trust. If societies are repeatedly exposed to manipulated content, the very basis of informed dialogue is undermined, which can have a ripple effect on public consensus/ perceptions. Disinformation can pose direct threats to democracy by for instance manipulating electoral processes, spreading false narratives about public figures, and influencing citizens' perception in governments. Indirectly, it could lead to public safety issues by spreading false information about health crises or stimulating violent actions/behaviours.

Journalism, Media and the Public Discourse

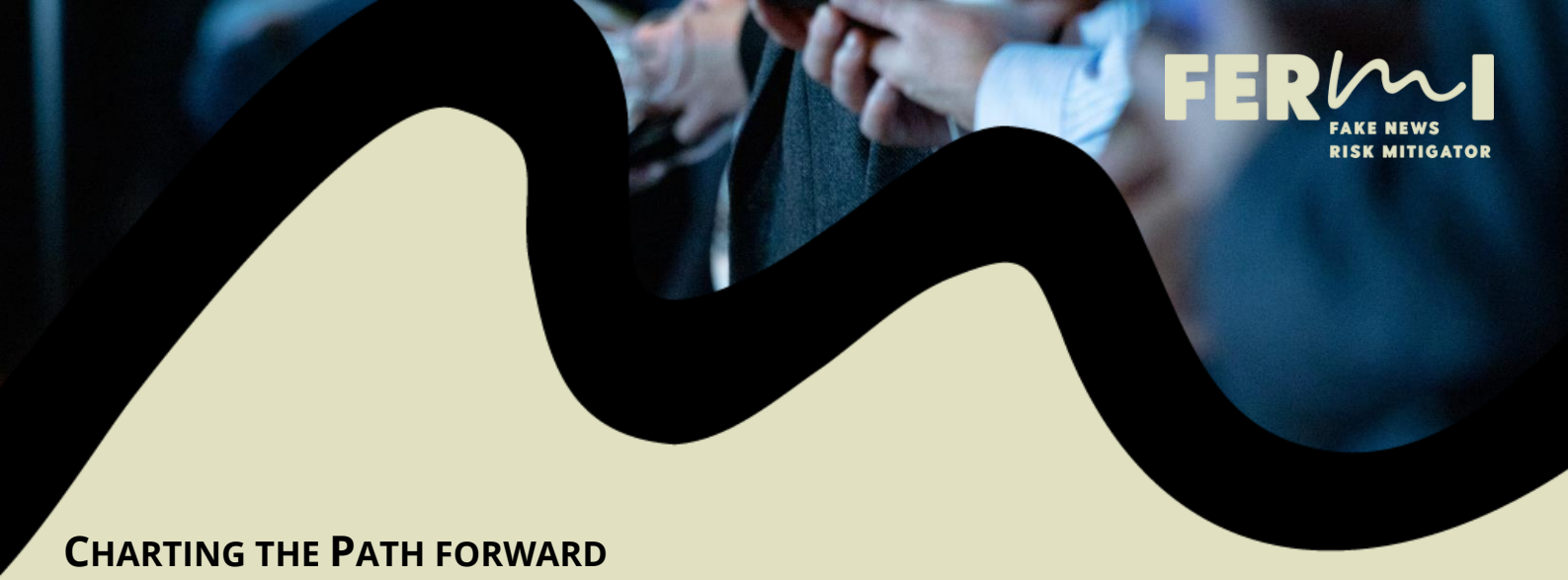
The digital age has severely impacted journalism and media consumption. We observe a shift to social media as the basic news source and this in turn has led to a crisis in traditional media business models leading to a precarious state for many media outlets. This rise of social media as a primary news source has led to increased competition for audience attention and this often comes at the expense of journalistic integrity. In response, journalists and media organisations are adopting new strategies to combat disinformation, including fact-checking services and investigative journalism. Furthermore, what has been reported is a growing trend of news avoidance, indicating societal exhaustion with the current state of information overload. This avoidance is disturbing and poses challenges not only to journalism but also to the very fabric of democratic engagement and political participation.

Countering Disinformation: A Multifaceted Approach

The legal and societal framework for addressing disinformation is an evolving landscape, it reflects the ongoing struggle to navigate the intersection of technology, law, fundamental rights and democratic values in the digital era. The environment in which disinformation flourishes is intricate and exploits the underlying vulnerabilities within societies. Disinformation does not exist in a vacuum, disinformation strategies are tailored to identify and magnify societal vulnerabilities/gaps, be they political, economic, cultural and so on. By echoing and exacerbating pre-existing biases and inequalities, disinformation finds fertile ground. There is an interplay between offline and online vulnerabilities thus any combating efforts must address both realms to be effective.

Collaborative Efforts and Future Directions

Technology indeed facilitates the spread of disinformation but it also offers tools to combat it. Artificial intelligence and machine learning algorithms can detect and flag various forms of disinformation with increasing accuracy. However, the reliance on technology to filter content raises ethical concerns about censorship and the potential for bias in algorithmic decision-making. Effective approaches to counter disinformation, therefore, must operate at the intersection of digital and societal resilience. This suggests that the need for media literacy and critical thinking skills and also fact-checking initiatives are paramount in building discerning and informed digital citizenry. Addressing the complexity of disinformation requires a multi-faceted approach. It calls for a 'whole society approach' where concerted efforts come from various levels of society and from both the public and private sphere, including government, tech companies, civil society, and the media. The call for identification and awareness-raising measures, conceptual clarity around trust and reliability, and tailored responses to various aspects of the disinformation challenge is only growing. In parallel, although regulation is vital, there should be a fine balance between implementing regulatory measures to combat disinformation and ensuring such measures do not supress freedom of expression and/or lead to excessive government control over media and information. We have to rely on collaborative and intersectional efforts which place at the forefront education, robust journalism and media literacy, and ethically oriented legal frameworks if we wish to foster a resilient information ecosystem within our societies.



Charting the Path forward

The challenging landscape of disinformation will continue to evolve along with technological advancements. Therefore, investing in education as well as in innovation in detection, is crucial in the effort of mitigating the impact of disinformation. Addressing disinformation is an ongoing process which necessitates adaptability, reflection, collaboration, and an ongoing commitment to upholding fundamental rights and democratic values.

As we reflect on the collective journey through the insights from the FERMI webinar and this document, we can only underscore the importance of collaborative efforts to uphold the integrity of information. It's clear that building digital trust and combating disinformation requires a concerted effort at different levels and from all sectors of society. Understanding and combating disinformation does not only revolve around regulatory measures, it is also prominently about furthering an informed and critical public capable of discerning 'truth' in the age of information overload.

Closing notes

This document has been produced by Convergence as the assigned Social Sciences and Humanities (SSH) partner of FERMI and task leader of "Training activities for all: Increasing understanding and digital trust" and is part of the training package material which complement the respective training activities undertaken throughout the project. In particular, this document has been drafted following the FERMI webinar "A dive into the societal landscape of disinformation - Balancing between Law Enforcement and Fundamental Rights to Increase Digital Trust" which took place on 23/02/2024. The aim of the training activity/webinar was to increase understanding of disinformation and digital trust. Two esteemed guest speakers presented their insightful views and research. The first guest speaker, Flavia Giglio,[2] focused on her legal research conducted on the EU legal framework on disinformation and the main fundamental rights challenges when adopting and enforcing counter-measures to it. The topic was further enriched by the second guest speaker, Carme Colomina[3], as a communication, security and geopolitics expert, and went beyond the FERMI context to the broader spectrum of the societal landscape of disinformation.

This final version of the document has been edited by Convergence based on the information and material derived from the FERMI webinar "A dive into the societal landscape of disinformation - Balancing between Law Enforcement and Fundamental Rights to Increase Digital Trust".

---

[2] Flavia Giglio: Legal Researcher in IT law, cybercrime and fundamental rights at the KU Leuven Center for IT & IP Law (CiTiP)
[3] Carme Colomina: Senior Research Fellow on European Union, disinformation and global politics at CIDOB (Barcelona Centre for International Affairs)

For Further Reading

This section can serve as a resourceful guide for individuals looking to expand their knowledge around the phenomenon of disinformation. Please note these are just a few suggestions/references from numerous, primarily drawn from the context of the FERMI webinar and relevant laws/initiatives/documents which comply and/or relate to the European Commission's guidelines.

- Bontcheva, Kalina, et al. *Balancing act: Countering digital disinformation while respecting freedom of expression*. Geneva, Switzerland: United Nations Educational, Scientific and Cultural Organization (2020).
- Charter of Fundamental Rights of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
- Colomina, Carme and Sánchez Margalef, Héctor, *Othering and Belonging in a Europe in crisis: narratives, identities, and the New-Old divide*. Democracy & Belonging Forum, 2022
- Colomina, Carme, et al., *The impact of disinformation on democratic processes and human rights in the world*. Brussels: European Parliament (2021): 1-19.
- Council of Europe, *Information Disorder: Toward an interdisciplinary framework for research and policymaking*, Available at: https://www.coe.int/en/web/freedom-expression/information-disorder
- Council of the European Union, Council conclusions on Complementary efforts to enhance resilience and counter hybrid threats, 14972/19, 2019. Available at: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf
- Council of the European Union, Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic, 14064/20, 2020. Available at: https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive).
- European Commission, Action Plan against Disinformation (Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018).
- European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling online disinformation: a European Approach, COM/2018/236 final, 2018. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

- European Commission, Directorate-General for Communication, (2019) Action Plan against disinformation : report on progress. Publications Office. Available at: https://data.europa.eu/doi/10.2775/18729
- European Commission, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Action Plan against Disinformation, JOIN(2018) 36 final, 2018. Available at: https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf
- European Commission, Tackling online disinformation, 2021. Available at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation
- European Convention of Human Rights (ECHR), Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG
- European Union, *Charter of Fundamental Rights of the European Union,* Official Journal of the European Communities,2000. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf
- European Union, *The Strengthened Code of Practice on Disinformation* (European Union, 2022). Available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
- Flore, M., *Understanding Citizens' Vulnerabilities: From Disinformation to Hostile Narratives,* EUR 30029 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-14307-9, doi:10.2760/276141, JRC118914. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC118914
- Giglio, Flavia. Moderation of illegal content and social media scraping. Privacy and data protection constraints in the processing of publicly available data by law enforcement authorities. i-Lex-Rivista di Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale 16.2 (2024): 17-33.
- Kalina Bontcheva and Julie Posetti (eds). *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*. Broadband Commission Research Report on Freedom of Expression and Addressing Disinformation on the Internet 2020. Available at: https://www.broadbandcommission.org/Documents/working-groups/FoE_Disinfo_Report.pdf
- Proposal (COD) 2021/0106 for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
- Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

FERMI
FAKE NEWS
RISK MITIGATOR

- The European Commission has developed a number of initiatives to tackle disinformation:
  - the Communication on ‘tackling online disinformation: a European approach’ is a collection of tools to tackle the spread of disinformation and ensure the protection of EU values;
  - the Action plan on disinformation aims to strengthen EU capability and cooperation in the fight against disinformation;
  - the European Democracy Action Plan develops guidelines for obligations and accountability of online platforms in the fight against disinformation;
  - The 2018 Code of Practice on disinformation was the first time worldwide that industry has agreed, on a voluntary basis, to self-regulatory standards to fight disinformation. It aimed at achieving the objectives set out by the Commission's Communication presented in April 2018
  - the COVID-19 disinformation monitoring programme, carried out by signatories of the Code of Practice, acted as a transparency measure to ensure online platforms’ accountability in tackling disinformation.
  - European Digital Media Observatory (EDMO) is an independent observatory bringing together fact-checkers and academic researchers with expertise in the field of online disinformation, social media platforms, journalist driven media and media literacy practitioners
  - the Strengthened Code of Practice on Disinformation, signed on 16th June 2022, brings together a wide range of players to commit to a broad set of voluntary commitments to counter disinformation

PARTNERS

Funded by the European Union

fighting-fake-news.eu