Law Enforcement Cooperation in the Prevention and Countering of Disinformation

Marius-Andrei OROȘANU
Police Academy ,,A.I. Cuza" Bucharest, Romania
andrei.orosanu@academiadepolitie.ro

Abstract

The growing impact of disinformation on public trust, democratic processes, and national security has made the prevention and countering of disinformation a strategic priority for law enforcement agencies. This paper explores the role of police cooperation -both national and international - in identifying, preventing, and responding to disinformation campaigns, particularly those amplified through digital platforms and social media. Law enforcement authorities, in collaboration with cybersecurity units, must adapt their operational frameworks to detect and address coordinated information manipulation. Romania, as a member of the European Union and signatory to multiple international agreements, actively participates in joint operations, data sharing, and institutional efforts through bodies such as Europol, Eurojust, and the European Centre of Excellence for Countering Hybrid Threats. Additionally, the involvement of civil society, media organizations, and private tech companies is essential for building resilience against disinformation. The paper argues that successful prevention requires a multidimensional approach: legal harmonization, technical capacity building, and the strengthening of cross-border cooperation mechanisms. In this context, Romania's growing institutional capability and engagement in EU-led initiatives underline its strategic role in the regional fight against disinformation.

Index terms: cybercrime, disinformation, European Union, hybrid attack, law enforcement cooperation

1. Introduction

In contemporary society, individuals are constantly exposed to a wide array of situations in which their responses are shaped by how they perceive what they see, hear, and read. Despite widespread access to education and digital technologies - many of which are specifically designed to support learning and self-directed knowledge acquisition - individuals are increasingly confronted with informational content that persuades them to accept presented narratives as inherently true.

This phenomenon has become particularly prominent in recent years, driven by several key factors: limited perceptual discernment, inadequate levels of formal education and self-education, an underdeveloped regulatory framework addressing information integrity, the complex and often manipulative nature of the media environment, and also the accelerated process and widespread dissemination of deceptive or misleading informational content.

These dynamics raise concerns regarding the public's ability to assess information, and they underscore the need for comprehensive strategies aimed at fostering media literacy, promoting institutional accountability, and strengthening individual resilience against disinformation.

In response to these challenges, national and international authorities have intensified their efforts to curb the spread of disinformation and promote critical thinking within the public sphere.

Through collaborative initiatives involving governmental institutions, educational systems, media organizations, and civil society, there is a growing emphasis on the importance of being accurately informed. These efforts aim not only to limit the reach of false or misleading content, but also to instill a culture of information verification, encouraging individuals to assess the credibility of sources before accepting or sharing information that may, directly or indirectly, impact their daily lives. The success of such initiatives depends largely on sustained public engagement and a shared understanding that being well-informed is both a personal responsibility and a societal necessity.

2. Definition and terminology

Disinformation, as a concept and term, is defined by competent institutional authorities as a harmful and growing phenomenon within society. It is understood as a form of strategic communication involving the deliberate dissemination of false or misleading information - whose inaccuracy can be objectively verified - with the purpose of obtaining economic gain or manipulating public opinion. The impact of such actions can lead to significant harm at the social, political, or institutional level, undermining democratic processes, public policymaking, and collective goods such as public health, security, or the environment. A piece of content may be classified as disinformation when the following essential criteria are cumulatively met:

- The information presented is false or misleading, and this nature can be objectively verified through reliable means of fact-checking.
- The intent behind its dissemination is either to secure economic gain or to deliberately manipulate public perception.
- The content possesses the potential to cause harm at a collective level, such as undermining democratic processes, compromising public safety, or eroding trust in state institutions.

The concept of disinformation, as defined at the European Union level, explicitly excludes certain forms of expression that, while potentially containing inaccuracies or provocative elements, do not fall within the scope of disinformation. These include:

- Satire and parody, recognized as legitimate forms of artistic expression and social commentary.
- Partisan commentary, provided it is clearly identifiable as such and does not involve deliberate deception.
- Editing or citation errors, which lack manipulative intent.
- Commercial advertising, which is regulated separately through specific legislation and self-regulatory codes within the advertising sector.

Although today's technological landscape is markedly different, understanding the concept of "informational dysfunction" requires a historical perspective on how information has been manipulated - through propaganda, strategic disinformation, satire, or hoaxes - as a persistent feature of the communication ecology. The term refers to a systemic imbalance in the information environment, wherein the boundaries between verified content and fabricated narratives become increasingly blurred, thereby impairing the public's ability to distinguish between genuine public-interest information and manipulative messaging.

Within this context, professional journalism plays a critical role in addressing such dysfunctions; however, it remains vulnerable, given that the development of journalistic standards is relatively recent when compared to the long-standing history of information manipulation [1].

The terms "fake news" and, more recently, "fake media" have undergone significant semantic distortion, being frequently misused to label information, institutions, or sources with which certain actors - often political - disagree, rather than referring to content that is factually incorrect, fabricated, or deliberately misleading. This improper usage has led to a conceptual erosion of the term,

undermining its analytical clarity and weakening the capacity to define and address harmful informational phenomena with precision. Data extracted from Google Trends indicate a marked increase in public interest for the term "fake news" beginning in the second half of 2016 - a period that coincides with its accelerated incorporation into global media and political discourse.

This analytical module aims, on one hand, to argue that the expression "fake news" is inadequate for capturing the complexity and scale of contemporary information pollution, and on the other hand, to underscore the problematic and potentially damaging consequences of its continued use in public discourse.

A key concern lies in the term's structural susceptibility to politicization and rhetorical manipulation. "Fake news" has increasingly been deployed as a discursive weapon - used to delegitimize media institutions, discredit professional journalism, and erode public trust in independent sources of information. In light of this trend, experts in public communication and information policy advocate for abandoning the term in favor of more precise and operationally valid concepts such as "disinformation" - the intentional dissemination of false information with manipulative intent - and "misinformation", which refers to the unintentional spread of inaccurate information absent deliberate intent to mislead [2].

3. The legal framework and its effectiveness in a rule-of-law state

In light of the accelerated development of digital technologies and the increased accessibility of informational content, including disinformation, EU Member States and their partner countries have recently established a more structured and legally coherent framework to address these challenges. Although earlier legal instruments - such as directives, regulations, and non-binding guidelines - existed, the current informational landscape demands centralized and systematic updates. Without such reform, societies remain vulnerable to high volumes of content that deviate from accepted standards of public discourse. As a result, intergovernmental legislative cooperation has been reinforced, and the existing legal architecture has undergone critical reassessment and targeted refinement to enhance both its efficiency and normative adequacy.

The present Regulation establishes a fully harmonised legal framework for intermediary services across the internal market, aiming to create a secure, transparent, and trustworthy online environment. It addresses the proliferation of illegal content and the broader societal risks posed by the dissemination of disinformation and other harmful materials, while ensuring the effective protection of fundamental rights as laid down in the Charter and promoting digital innovation. Consequently, Member States are precluded from introducing or upholding national provisions in areas covered by this Regulation, unless explicitly authorised to do so. Such unilateral measures would risk undermining the uniform and direct application of the harmonised rules governing intermediary service providers. However, this does not exclude the possibility for Member States to enforce other national laws - consistent with Union law, including Directive 2000/31/EC, particularly Article 3 - where those laws pursue legitimate public interest objectives distinct from those addressed by this Regulation.

The Regulation categorizes the risks related to disinformation into four principal groups. These encompass:

- The first category of risks involves the spread of illegal content such as child sexual abuse material, unlawful hate speech, and other criminal uses of online services. It also includes the trade of illegal goods like counterfeit products and illicit animal trafficking. These activities pose systemic risks, especially when amplified by widely influential accounts or mechanisms. Very large online platforms and search engines must assess these risks, regardless of their terms of service. This risk assessment does not affect the legal liability of users or website operators under applicable law.

- The second category concerns the impact of digital services on fundamental rights protected by the EU Charter, including human dignity, freedom of expression, privacy, non-discrimination, children's rights, and consumer protection. Risks can stem from algorithm design or abusive practices such as malicious takedown notices or silencing users. Providers must especially address risks to minors, including exposure to harmful or addictive content and unclear platform design.
- The third category relates to adverse effects on democratic processes, civic discourse, electoral integrity, and public safety. This includes information manipulation and amplification of harmful narratives by large platforms and search engines, which can distort elections, undermine public debate, and weaken trust in democratic governance, threatening social cohesion and political stability.
- The fourth category covers risks from platform design, operation, or manipulative use impacting public health, minors' welfare, and individual physical and mental well-being, including gender-based violence. These risks arise from disinformation campaigns on health issues or addictive interface designs that exacerbate vulnerabilities and harm.

Understanding these categories is essential for developing targeted regulatory responses aimed at mitigating the multifaceted challenges posed by disinformation in the digital age [3].

4. Applicability and cooperation among authorities

In Romania, this initiative has been materialized through Law No. 50/2024, published in the Official Gazette No. 232 on March 19, 2024, and entering into force on March 22, 2024. The purpose of this law is to establish the institutional, procedural, and sanctioning framework necessary for the effective national implementation of the Digital Services Act (DSA) and to harmonize relevant national legislation - notably Law No. 365/2002 on electronic commerce - with the requirements of the new European framework.

The adoption of Law No. 50/2024 was driven by a series of both internal and external factors. Firstly, the obligations arising from European Union law were fundamentals in this case. As an EU regulation, the DSA is directly applicable in all Member States, but requires institutional and organizational measures to ensure its practical enforcement. Secondly, Romania previously lacked a coherent legal framework regarding the oversight of intermediary digital services. Legislative gaps posed the risk of inconsistent or inefficient application of the new obligations. Finally, the evolution of e-commerce, the emergence of new forms of illegal content, and the multiplication of systemic disinformation cases have increased the pressure for clear legislative intervention.

Law No. 50/2024 aims to establish the measures necessary to implement the DSA at the national level. It covers both the institutional organization (through the designation of competent authorities) and the procedures for oversight and enforcement applicable in cases of non-compliance with the regulation's provisions. The law also amends and supplements Law No. 365/2002 on electronic commerce in order to align it with the new European legislative framework.

The regulation applies to intermediary service providers operating within Romanian territory or having a legal representative established in Romania. This ensures legal coverage for both domestic platforms and international actors targeting users in Romania.

At the core of the institutional architecture established by the law is ANCOM (The National Authority for Management and Regulation in Communications), which is legally designated as the Digital Services Coordinator in Romania. This designation places ANCOM at the center of the supervisory, enforcement, and implementation process of DSA provisions. Among ANCOM's responsibilities are:

- Monitoring the compliance of intermediary service providers with their obligations.

- Imposing corrective measures or sanctions.
- Collaborating with relevant authorities in Romania and other Member States.
- Evaluating applications for the recognition of the status of "vetted researcher" for access to platform data.
- Acting as the single point of contact for information exchange with the European Commission and other national authorities.

In addition to ANCOM, the law introduces the concept of a "relevant authority", which includes public or judicial institutions empowered to issue legally binding orders to platforms-for instance, to remove illegal content or provide specific data. The law mandates a cooperation obligation between the Digital Services Coordinator and these authorities, through the exchange of information, consultation, and formal cooperation agreements.

A core aspect of Law No. 50/2024 is the establishment of clear obligations for intermediary service providers, in alignment with the provisions of the DSA. These obligations include:

- Submitting a notification to ANCOM within 45 days of commencing operations, providing identification data and a contact person.
- Notifying ANCOM of any subsequent changes within 10 days.
- Ensuring mechanisms for reporting illegal content.
- Cooperating with authorities by providing data and complying with imposed measures.
- Observing transparency requirements, including the publication of reports on content moderation and online advertising activities.

Providers that fail to comply or refuse to cooperate may be subject to corrective measures and significant administrative sanctions, in accordance with the regime established by the law and the DSA. To ensure effective enforcement of the legal provisions, Law No. 50/2024 establishes a robust sanctioning framework. ANCOM has the authority to impose proportionate, dissuasive, and, in some cases, cumulative administrative fines. Offenses may include:

- Failure to notify the authorities.
- Non-compliance with transparency obligations.
- Refusal to cooperate during inspections or in response to official requests.

The law allows for the contestation of inspection reports and sanctioning decisions within 15 days before the competent court. Furthermore, reports may be issued in electronic format and communicated via digital platforms (e.g., "My ANCOM"), in line with the principles of digitalization and administrative efficiency.

An innovative element of the law is the regulation of access to data for researchers. ANCOM may accredit individuals or institutions as "vetted researchers", thereby allowing access to relevant data from Very Large Online Platforms (VLOPs). Such data is essential for assessing the societal impact of digital content, identifying systemic risks, and formulating evidence-based public policies.

This provision aligns with the DSA's objective to encourage academic research and the involvement of civil society in the ongoing monitoring of the digital environment.

Amendments to Law No. 365/2002

Law No. 50/2024 introduces several important amendments to Law No. 365/2002 on electronic commerce, including:

- Alignment of definitions and terminology.
- Completion of provisions regarding the liability of service providers.
- Adjustment of the sanctioning regime to comply with DSA standards.

Through these modifications, the Romanian legal framework governing electronic commerce becomes fully compatible with the European standards on digital services [4].

The Ministry of Internal Affairs (MAI) of Romania stand against disinformation, holding clearly defined institutional and operational responsibilities. These duties are established through

various normative acts and materialize through specific actions carried out by the MAI's structures. MAI operates in accordance with national and European legislation, including Regulation (EU) 2022/2065 on digital services (Digital Services Act - DSA). Within this context, MAI cooperates with other public and private institutions to ensure the effective implementation of measures aimed at combating disinformation.

MAI undertakes specific activities to prevent and counter disinformation, including:

- Online Environment Monitoring which means Identification and reporting of manipulative content, including the use of technologies such as deepfake. For example, in 2025, MAI identified a Tik-Tok account disseminating videos generated with artificial intelligence aimed at discrediting a candidate for the Romanian presidency [5].
- Collaboration with Online Platforms in terms of reporting accounts and materials that violate community standards or national legislation to prevent the spread of disinformation.
- Public Information such as providing accurate and verified information through official channels to counteract false news and educate citizens on identifying such content.

MAI collaborates with various national and international institutions to combat disinformation such as the National Authority for Administration and Regulation in Communications (ANCOM) to implement national and European regulations and with organizations like Europol and Interpol to address cross-border disinformation and exchange best practices.

The Romanian Police Force, under the coordination of MAI, has specific duties in combating disinformation which implies investigation of cybercrimes defined by identifying and sanctioning individuals who disseminate false information with the intent to induce panic or manipulate public opinion [6]. Also, acts for prevention of cybercrime conducting public information and education campaigns to prevent victimization via the internet.

For educational purposes, MAI implements educational programs aimed at increasing public awareness regarding the dangers of disinformation and establish partnerships with Media [7].

Reference case analysis

On the evening of March 9, 2025, Romania confronted a coordinated disinformation campaign disseminated predominantly via social media platforms, aiming to distort public perception regarding public order events occurring that day. The propagation of fabricated information posed a significant risk to social cohesion and public trust in state institutions. This case study explores the characteristics of the disinformation, the institutional mechanisms activated in response, and the efficacy of the measures undertaken by Romanian authorities to protect the public from misleading information and its detrimental effects.

The widespread adoption of digital communication technologies has increased societal exposure to disinformation campaigns. These campaigns frequently exploit social tensions to manipulate public opinion, potentially undermining social stability and institutional credibility. The events of March 9, 2025, in Romania, serve as a pertinent illustration of such a phenomenon. On this date, distorted and unfounded information concerning law enforcement activities circulated extensively, eliciting a concerted institutional reaction.

During the evening hours of March 9, multiple social media posts and videos surfaced, alleging disproportionate or unlawful actions by law enforcement agencies during public gatherings. Some materials included manipulated images and videos, which were widely disseminated and amplified within various online communities. The intent of this disinformation campaign was to delegitimize the police and gendarmerie, while fostering a generalized distrust toward public authorities. The Romanian Ministry of Internal Affairs, through its operational bodies including Romanian Police and Romanian Gendarmerie, implemented a coordinated response aimed at mitigating the effects of the disinformation.

Fig. 1. https://www.facebook.com/www.politiaromana.ro/

The response comprised several key components:

- Public communication and transparency - Authorities issued official statements clarifying factual circumstances, rectifying misleading narratives, and disseminating verified information to the public. This approach was instrumental in restoring institutional credibility and preventing the escalation of social tensions.
- Investigation and legal actions - Specialized cybercrime units within the Romanian Police initiated inquiries to identify the originators of manipulated content and individuals orchestrating the disinformation efforts. Where appropriate, legal actions were pursued for offenses related to spreading false information and incitement.
- Collaboration with digital platforms - The authorities engaged in sustained cooperation with social media companies to identify, flag, and remove content deemed harmful or misleading, thereby limiting its dissemination.
- Inter-institutional coordination - The MAI coordinated efforts with other pertinent agencies, such as the National Authority for Management and Regulation in Communications (ANCOM) and intelligence services, to monitor the digital landscape continuously and anticipate emerging disinformation threats [8].

The comprehensive and transparent intervention by Romanian authorities contributed to attenuating the societal impact of the disinformation campaign. The dissemination of accurate and timely information counterbalanced false narratives before they could substantially influence public opinion or provoke unrest. Furthermore, the initiation of criminal investigations signified a firm institutional stance against the manipulation of public information.

This case exemplifies the efficacy of a multifaceted approach, combining informed public communication, rigorous investigative procedures, and collaborative engagement with private sector actors in the digital domain. It also underscores the imperative of sustained vigilance and preparedness to address the evolving modalities of disinformation campaigns.

The events of March 9, 2025, highlight the challenges inherent in combating disinformation in the contemporary information environment and demonstrate the capacity of Romanian authorities to mobilize institutional resources effectively to protect public trust and informational integrity. Ongoing efforts to enhance legal frameworks, institutional capabilities, and public awareness remain vital for the continued resilience against disinformation phenomena.

5. Conclusion

Addressing the phenomenon of disinformation presents a multifaceted challenge that requires a coordinated and integrated response from police structures, alongside other public authorities and

digital environment stakeholders. Recent experiences illustrate that an effective prevention and response system relies on the timely and transparent exchange of information, inter-institutional cooperation, and the utilization of advanced technologies for monitoring and analyzing online content. The role of law enforcement extends beyond investigating and sanctioning those who deliberately disseminate false information; it also encompasses fostering public trust through clear and verified communication.

To enhance the effectiveness of actions against disinformation, it is advisable to strengthen bilateral and multilateral collaboration mechanisms between national police forces, European institutions, and digital platforms. The development of joint specialized training programs, as well as integrated digital platforms for data exchange and best practices, would contribute to a more coordinated and efficient response. Moreover, involving civil society and academia in monitoring and educational processes can amplify the positive impact of law enforcement interventions.

Consequently, police cooperation constitutes a foundational element within the complex framework of combating disinformation, contributing to the safeguarding of informational security.

References

[1]. European Commission, 16 JUNE 2022, "2018 Code of Practice on Disinformation", Available: 2018 Code of Practice on Disinformation | Shaping Europe's digital future.

[2]. UNESCO, 2018 "Journalism, fake news & disinformation: handbook for journalism education and training", Available: https://unesdoc.unesco.org/ark:/48223/pf0000265552.

[3]. European Parliament and Council, 19 October 2022, "Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)." Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065.

[4]. Romanian Parliament, 18 March 2024, "Legea nr. 50 din 18 martie 2024 privind stabilirea unor măsuri pentru aplicarea Regulamentului (UE) 2022/2.065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale), precum și pentru modificarea și completarea Legii nr. 365/2002 privind comerțul electronic", Available: LEGE 50 18/03/2024 - Portal Legislativ.

[5]. Romanian Ministry of Internal Affairs, 18 May 2025 "Comunicat de presă privind identificarea și raportarea unui cont de social media care difuzează conținut manipulator de tip deepfake", Available: https://www.mai.gov.ro/comunicat-de-presa-privind-identificarea-si-raportarea-unui-cont-de-social-media-care-difuzeaza-continut-manipulator-de-tip-deepfake/.

[6]. Romanian Ministry of Internal Affairs, 20 January 2015, "Vizită de evaluare a activităţii de combatere a criminalităţii informatice din România", Available: https://www.mai.gov.ro/vizita-de-evaluare-a-activitatii-de-combatere-a-criminalitatii-informatice-din-romania/.

[7]. Romanian Ministry of Internal Affairs, 7 February 2025 "Navigare responsabilă pe internet. Cum putem preveni riscurile în mediul online", Available: https://www.mai.gov.ro/navigare-responsabila-pe-internet-cum-putem-preveni-riscurile-in-mediul-online/.

[8]. Juridice.ro, 10 March 2025, "Poliția Română anunță că pe TikTok/Facebook se desfășoară o campanie de dezinformare ref. protestul din 9 martie 2025", Available: https://www.juridice.ro/774393/politia-romana-anunta-ca-pe-tiktok-facebook-se-desfasoara-o-campanie-de-dezinformare-ref-evenimentele-din-9-martie-2025.html.