Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Review Article

CRIMINAL LIABILITY FOR PAID DISINFORMATION IN THE DIGITAL WORLD: A COMPARATIVE STUDY BETWEEN UAE LAW AND THE EUROPEAN DIGITAL SERVICES ACT (DSA)

Mohammad Amin Alkrisheh* and Fatiha Mohammed Gourari

ABSTRACT

Background*: With the rapid digital transformation and the extensive use of social media platforms, disseminating various forms of harmful digital content—including illegal content and false or misleading information, particularly when financially incentivised—has become a pressing global challenge. These practices threaten digital trust and pose significant risks to societal stability. Despite the growing legal efforts to address these crimes, a unified and comprehensive legal framework remains lacking. This study examines the criminal liability associated with paid disinformation in the digital world, comparing the legal approach under UAE law with the European Digital Services Act (DSA). While the UAE has enacted specific provisions targeting the monetisation of disinformation, the European framework primarily focuses on the responsibilities of digital platforms without explicitly addressing individual actors involved in such activities.*

Methods: *This study employs a comparative legal analysis, focusing on relevant legislative provisions in both jurisdictions. The research applies an analytical and comparative approach, examining Article 55 of the UAE's Anti-Rumours and Cybercrime Law, which explicitly criminalises financial incentives for disseminating illegal content. In contrast, the study assesses the European DSA, which primarily regulates platform accountability but lacks direct provisions on individual criminal liability for paid disinformation. The analysis also incorporates doctrinal legal research and case studies to highlight the effectiveness and limitations of each legal system in combating this issue.*

Results and Conclusions: *The study finds that UAE law provides a more structured and detailed legal framework for addressing paid disinformation, offering clear criminal sanctions for individuals engaged in such acts. Conversely, the European DSA adopts a broader regulatory approach, focusing on institutional oversight without directly addressing the criminal liability of individuals involved in monetised disinformation. The research recommends that European legislation adopt a more specific model to combat these crimes, integrating direct criminal accountability alongside platform regulation. Additionally, the study emphasises the need for enhanced international cooperation and regulatory harmonisation to strengthen digital transparency and mitigate the risks posed by financially motivated disinformation.*

1 INTRODUCTION

The digital world has undergone rapid and transformative developments in exchanging and disseminating information. Social media platforms and other digital tools now play a pivotal role in shaping public opinion and influencing various political, social, and economic aspects of life. Alongside these advancements, serious legal and ethical challenges have emerged—particularly concerning false and misleading information. The phenomenon of "paid disinformation" is of growing concern, where such content is intentionally spread in exchange for financial or moral incentives, posing threats to societal stability and undermining public trust in the digital environment. Studies have shown that emerging technologies such as deepfake videos and generative artificial intelligence significantly amplify the scale and credibility of such disinformation, making legal regulation increasingly complex.[1]

This research focuses on criminal liability for paid disinformation in the digital world. It analyses the approach taken by UAE law, which establishes a comprehensive legal framework to combat this phenomenon under the UAE Anti-Rumours and Cybercrime Law. It also compares this to the European Digital Services Act (DSA), which primarily regulates the responsibilities of digital platforms. At the same time, criminal liability for individuals remains under the jurisdiction of member states' national legislation. This distinction has raised concerns among legal scholars about potential gaps in accountability.[2]

1. Achhardeep Kaur and others, 'Deepfake Video Detection: Challenges and Opportunities' (2024) 57(6) Artificial Intelligence Review 159, doi:10.1007/s10462-024-10810-6; Raghu Raman and others, 'Fake News Research Trends, Linkages to Generative Artificial Intelligence and Sustainable Development Goals' (2024) 10(3) Heliyon e24727, doi:10.1016/j.heliyon.2024.e24727.
2. Marc Tiernan and Goran Sluiter, 'The European Union's Digital Services Act and Secondary Criminal Liability for Online Platform Providers: A Missed Opportunity for Fair Criminal Accountability?' (*SSRN*, 18 March 2024) doi:10.2139/ssrn.4731220 <https://ssrn.com/abstract=4731220> accessed 25 February 2025.

Given the global exploitation of social media to influence public opinion and shape narratives, the need to protect the digital environment from the risks associated with paid disinformation has become increasingly urgent. Recent studies have shown that artificial intelligence technologies, particularly deepfakes and generative AI models, have significantly increased the sophistication and reach of disinformation, complicating legal responses to such content.[3] This study is significant because it examines how UAE law addresses crimes related to paid disinformation in the digital world. It highlights the legal mechanisms established by the Emirati legislative framework to criminalise individual behaviours associated with these offences. It also sheds light on the regulatory aspects of the European Digital Services Act (DSA), particularly its platform-focused approach. While the DSA aims to regulate systemic risks, legal scholars have noted its lack of direct criminal provisions for individual accountability, raising questions about the effectiveness of its enforcement model.[4]

The research problem centres on legislators' legal challenges in combating paid disinformation in the digital world, which poses significant threats to societal stability and digital information security. This study explores the extent to which the **UAE legislator** has succeeded in establishing a comprehensive legal response to such crimes and contrasts this with the European Digital Services Act (DSA), which provides a regulatory framework focusing primarily on digital platforms' responsibilities while leaving criminal liability for individuals to the discretion of national laws in EU member states. The research further examines the limitations and strengths of both systems and proposes legal mechanisms that could enhance the effectiveness of efforts to combat paid disinformation in the digital environment.

2 RESEARCH METHODOLOGY

This study adopts an analytical approach to legal texts, focusing on the relevant legislative provisions governing paid disinformation in the United Arab Emirates (UAE) and the European Union (EU). The research examines Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes in the UAE, particularly Article 55, which explicitly criminalises the acceptance of financial incentives for disseminating illegal content. Additionally, it analyses the European Digital Services Act (DSA), which establishes a regulatory framework for online platforms but does not contain explicit provisions criminalising individuals engaged in the monetisation of disinformation.

A comparative legal method is employed to identify similarities and differences between the UAE and EU legal frameworks, exploring the legislative approaches adopted in both jurisdictions and the extent to which they address the criminal liability of individuals involved in paid disinformation. The study analyses the definitions of key legal concepts,

3. Kaur and others (n 1) 159; Raman and others (n 1) 3.
4. Tiernan and Sluiter (n 2) 14.

including "illegal content" and "false or misleading information," as interpreted within each legal system. Furthermore, relevant jurisprudence and doctrinal legal interpretations are analysed to clarify the scope of criminal liability associated with these offences. The study also scrutinises the constitutive elements of the offence of accepting financial incentives to spread false or illegal content and assesses the penalties prescribed under both legal frameworks.

By highlighting legislative gaps within the European framework, the research demonstrates that while the UAE legal system provides a more direct and explicit criminalisation of paid disinformation, the European DSA primarily focuses on the regulatory responsibilities of digital platforms rather than imposing individual criminal liability. The analysis further examines how criminal conduct is defined and liability is assigned under each legal system, offering insights into the effectiveness of existing legal mechanisms in addressing this phenomenon. The study concludes by synthesising the key findings and proposes recommendations to strengthen legal responses to disinformation monetisation, enhance regulatory coherence, and promote digital transparency.

3 MISLEADING INFORMATION AS A FORM OF ILLEGAL CONTENT

To understand the dimensions of criminal liability for paid disinformation in the digital world, it is essential first to define the concepts of "illegal content," "false information," and "paid disinformation," as these constitute the foundational elements of the crime of receiving an incentive to disseminate unlawful or misleading material.

False or misleading information is considered illegal when it violates legal standards, especially when its publication harms public order, national security or the spread of baseless rumours. Illegal content broadly refers to any material or expression contravening the law, including hate speech, terrorism-related content, or harmful falsehoods. In this context, paid disinformation describes publishing or republishing such content in exchange for financial or moral benefits. Clarifying these definitions is crucial for understanding the legal treatment of such acts under UAE law and the European Digital Services Act (DSA).

3.1. The Concept of Illegal Content

Illegal content is one of the most ambiguous legal notions, as its definition and standards vary across different countries' legal, cultural, and political systems. Due to the international nature of the Internet, this term exhibits significant divergence in interpretation among nations, creating a substantial challenge in unifying the standards for addressing such content.[5]

5 Majid Yar, 'A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media' (2018) 1(1) International Journal of Cybersecurity Intelligence & Cybercrime 5, doi:10.52306/01010318RVZE9940.

Defining illegal content is a fundamental step in understanding the scope of digital crimes, especially in the context of paid disinformation or the dissemination of false information. This concept is significant due to the global nature of the Internet and the divergence in legal systems across countries. While legislators aim to establish clear definitions, challenges persist due to the dynamic nature of digital content.[6]

The UAE legislator has explicitly defined the concept of illegal content in Article 1 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes.[7] Unlawful content is described as: "Content that constitutes the subject of a punishable crime under the law, or whose publication, circulation, or re-circulation within the state may harm the state's security, sovereignty, or any of its interests; public health; public order; friendly relations with other states; or influence the results of elections for the Federal National Council or advisory councils in the emirates. It may also incite hostility or hatred between different groups of people, lower public confidence in the performance of any duty or task, or affect the exercise of authority by state entities or any of its institutions."

This definition highlights the comprehensive scope of illegal content under UAE law, addressing various dimensions of harm that could arise in the digital environment.

In addition, Article 3 (h) of the European Digital Services Act (DSA) defines illegal content as: "Information that, in itself or about an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State that complies with Union law, irrespective of the precise subject matter or nature of that law."[8]

This definition emphasises content alignment with national and European laws, assigning digital platforms the responsibility to monitor and remove non-compliant content. It exhibits flexibility by allowing the specific details of illegal content to be determined by the national laws of each Member State. Examples of illicit content under the DSA include:

- Hate speech and incitement to violence.
- Promotion of terrorism or related materials.
- Exploitation of children and unlawful sexual content.
- Violations of intellectual property rights.
- Dissemination of disinformation that undermines public order or societal safety.

6 Khawlah M AL-Tkhayneh, Abdulrasheed Olowoselu and Mohammad Amin Alkrisheh, 'The Crime in Metaverse (The Future Scenarios for Crime Patterns and the Prospective Legal Challenges)' (2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, UAE, November 2023) doi:10.1109/SNAMS60348.2023.10375402.

7 Federal Decree-Law no (34) of 2021 'On Combating Rumours and Cybercrimes' [2021] Official Gazette of UAE 712.

8 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)' [2022] OJ L 277/1.

The phenomenon of paid disinformation is not limited to political or social manipulation; it also extends into the commercial domain, where individuals or entities intentionally publish misleading content for financial gain. One typical example is deceptive online advertising, which shares core characteristics with criminally relevant disinformation—namely, the intent to mislead and the presence of economic incentives.[9]

In this context, some legal commentators distinguish between illegal and unsafe content. Illegal content explicitly violates statutory provisions—for example, inciting violence, disseminating hate speech, or publishing false information that threatens public order. By contrast, unsafe content refers to materials that may not breach legal thresholds but still pose risks to platform integrity, public confidence, or brand reputation. This differentiation underscores the broader regulatory and ethical considerations that digital platforms and legislators must address in maintaining a safe, reliable, and lawful digital environment.

Some legal scholars argue that illegal content should be defined based on its nature and impact. They describe it as the opposite of legitimate, purposeful, and lawful content – inappropriate for publication and offensive to public taste and morals. This includes disseminating irresponsible words, images, or comedic videos that lack awareness, often descending into triviality and violating societal norms and traditions. It has also been defined as:

- "Any act or behaviour related to creating and disseminating content that disrupts public morals or offends public taste."[10]
- "The production of short video materials that spread online and include songs, acting, comedic content, and satirical commentary, some of which contain obscene language accompanied by physical gestures or dancing, as well as addressing controversial social topics such as gender relations and family issues in a predominantly conservative environment."[11]

These definitions highlight the broader cultural and societal considerations in determining illegal or inappropriate content, reflecting the influence of prevailing social values and traditions in shaping legal and ethical standards for digital content.

9 Tariq Abdel Rahman Kameel, Moustafa Elmetwaly Kandeel and Mohammad Amin Alkrisheh, 'Consumer Protection from Misleading Online Advertisements "An Analytical Study in UAE Law"' (2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, UAE, November 2022) doi:10.1109/ACIT57182.2022.9994108.

10 Ashour Abdel Rahman Ahmed Mohamed, 'Civil Responsibility For Providers Of Illicit Content Circulating On The Internet (A Comparative Study Between French Law And Egyptian Law)' (2020) 35(3) Journal of the Faculty of Sharia and Law, Tanta University 1098, doi:10.21608/mksq.2020.111506.

11 Mahmoud Mohammed Abu Farwa, 'Social Media Platforms and Their Legal Liability for Illegal Content' (2022) 39 Kuwait International Law School Journal 175.

It has also been defined as content that includes information in any form—images, videos, writing, or gestures—that is violent, incites violence, is sensitive or inappropriate, or encourages any criminal activity or promotes unsafe behaviour.

The principle of public order plays a significant role in determining the legality of content disseminated through social media. Content that violates public order in all its aspects—economic, political, social, religious, and public morals—is considered illegal content. Consequently, harmful content is indistinguishable from unlawful content, as both undermine societal stability and contravene established norms and standards.[12]

Some scholars believe that defining illegal content depends on identifying actions that exceed the boundaries of freedom of expression and negatively impact public order, such as incitement to violence,[13] hate speech and media manipulation. The lack of international consensus on this term presents a significant challenge in combating its spread across digital platforms.[14]

This perspective highlights the delicate balance between protecting freedom of expression and maintaining societal stability, emphasising the need for a unified approach to address the complexities of illegal content in a globally interconnected digital environment.

The rulings issued by the European Court of Justice (ECJ) demonstrate that European jurisprudence has not provided a comprehensive and precise definition of illegal content. Instead, it has addressed specific manifestations of such content in applying European legislation. For instance, in the *Right to Be Forgotten* case (2019),[15] the Court discussed individuals' rights to request the removal of irrelevant or excessive content. Still, it did not establish a universal definition for illegal content. Similarly, other cases, such as the *YouTube* Case (2020),[16] which focused on data protection, and the *Planet49* Case (2019),[17] which dealt with cookie consent and privacy violations, emphasised specific legal issues

12 Amhamed Al-Mansouri, 'Publishing and Promoting Fake News between the Criminal Law and the Press and Publishing Law' (2024) 13 Electronic Journal of Legal Research 258 <https://revues.imist.ma/index.php/RERJ/article/view/47387> accessed 25 February 2025.

13 Mohammad Amin Alkrisheh, Saif Obaid Al-Katbi and Khawlah M Al-Tkhayneh, 'The Criminal Confrontation for Crimes of Discrimination and Hate Speech: A Comparative Study' (2024) 7(2) Access to Justice in Eastern Europe 138, doi:10.33327/AJEE-18-7.2-a000210; Hassan Mohamed Ahmed Hassan, 'Media Publication Crimes: A Comparative Jurisprudential Study with Positive Law – The Crime of Incitement as a Model' (2024) 47 Journal of Jurisprudential and Legal Research 487.

14 Yar (n 5).

15 *Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL)* Case C-507/17 (CJEU, 24 September 2019) <https://curia.europa.eu/juris/liste.jsf?num=C-507/17> accessed 25 February 2025.

16 *Constantin Film Verleih GmbH v YouTube LLC and Google Inc* Case C-264/19 (CJEU, 9 July 2020) <https://curia.europa.eu/juris/liste.jsf?num=C-264/19> accessed 25 February 2025.

17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* Case C-673/17 (CJEU, 1 October 2019) <https://curia.europa.eu/juris/liste.jsf?num=C-673/17> accessed 25 February 2025.

like privacy and intellectual property rights without directly addressing the broader concept of illegal content.

This approach reflects the European courts' reliance on regulations such as the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR) to define the legal framework for illegal content. These regulations delineate the scope of unlawful content based on violating national or European laws. Thus, the role of the ECJ primarily involves interpreting and applying these laws rather than formulating a comprehensive legal definition of illegal content.

It is important to note that addressing illegal content in the context of media disinformation requires precise and well-defined terminology, given the cross-border nature of this phenomenon. The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression emphasised this necessity in their 2021 report to the Human Rights Council. The report underscored the importance of developing clear definitions of illegal content to tackle the challenges posed by media disinformation.[18]

3.2. The Concept of False Information

False or misleading information has sparked widespread debate in the digital age due to its significant social, political, and economic impacts. This study uses the term to reflect entirely fabricated content and information that may be partially true but presented in a deceptive or manipulated context. Definitions of false information vary across legal, cultural, and social systems. Describing a piece of news or information as "false" is often complex, as it depends heavily on subjective and artistic standards, making it challenging to establish a comprehensive and precise definition.

False information frequently intersects with misleading news or content that aims to mislead the public, blurring the lines between intentional deception and unintended inaccuracies.[19] This ambiguity underscores the difficulties in setting universal criteria for identifying and addressing false information across different jurisdictions.

The UAE law defines false information in Article 1 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes as: "Rumours and false or misleading statements, whether wholly or partially false, and whether by themselves or in the context in which they appear."[20]

18 Irene Khan, 'Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (UN 2021) <https://digitallibrary.un.org/record/3925306?ln=en> accessed 25 February 2025.

19 Raman and others (n 1); Anja Hoffmann and Alessandro Gasparotti, *Liability for Illegal Content Online: Weaknesses of the EU Legal Framework and Possible Plans of the EU Commission to Address them in a "Digital Services Act"* (CEP 2020).

20 Federal Decree-Law no (34) of 2021 (n 7) art 1.

This definition highlights the emphasis placed by UAE legislators on the intent to mislead, whether the information is entirely false or merely misleading within its context or framing. It highlights that both the content and the manner in which it is presented are relevant in determining legality.

False information can take various forms, depending on the deceptive intent behind its production, including:[21]

1. Fabricated Content: Entirely false content, significantly diverging from the truth.
2. Impersonated Content: Involves identity theft of genuine sources.
3. Misleading Content: Information presented in a way that falsely accuses or misdirects against individuals, entities, or issues.
4. Manipulated Content: Edited or doctored materials, such as cut-and-paste modifications, designed to create a false impression.
5. False Context: Accurate information placed within a false framework or context, leading to public deception.
6. False Association: Using unrelated headlines or images to misrepresent the actual content.
7. Satire or Parody: Although not directly harmful, these can indirectly mislead audiences or propagate false information subtly.
8. Deepfakes: Content created using artificial intelligence to produce compelling but entirely fabricated material.[22]

Conversely, the European Digital Services Act (DSA) does not provide a specific definition of false information as a standalone phenomenon. However, it addresses the dissemination of illegal content, which may include false information if its spread causes societal harm or violates European or national laws. The DSA primarily focuses on the responsibility of digital platforms, rather than individual accountability.

False information is also addressed more broadly under the European Union's strategies for combating media disinformation. Examples under the DSA include:[23]

- Fake News: Deliberately false information aimed at influencing public opinion.

21 Ahmed Gamal Hassan Mohammed, 'Mechanisms of the Egyptian Public in Verifying Fake News and its Relationship their Interactive Patterns on Social Networking Sites' (2021) 59(2) Journal of Media Research 1008, doi:10.21608/jsb.2021.199620; Mohammed Salem Alneyadi and others, 'The Crime of Electronic Blackmail in the Emirati Law' (2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, UAE, November 2022) doi:10.1109/ACIT57182.2022.9994165.

22 Kaur and others (n 1) 159.

23 EU, 'A Europe that Protects: The EU Steps up Action against Disinformation: Press release' (*European Commission*, 5 December 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6647> accessed 25 February 2025; EU, 'The Strengthened Code of Practice on Disinformation 2022' (*European Commission*, 16 June 2022) <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> accessed 25 February 2025.

- Misleading Context: Accurate information presented within deceptive or manipulated contexts.
- Deepfakes: Content created using artificial intelligence to produce compelling but entirely fabricated material.

The European Media Disinformation Centre defines false information as: "Any content intentionally designed to mislead or manipulate public opinion through technical means such as deepfake technology."[24]

From the above, it is evident that UAE law provides a clear and precise definition of illegal content and false information, treating it as a standalone offence. In contrast, European law adopts a less detailed approach, offering a general definition of unlawful content and leaving the specific legal nuances to be applied by individual Member States under their national laws. The European framework emphasises the regulation of internet platforms rather than the content itself.

To enhance the effectiveness of the Digital Services Act (DSA), it is suggested that the regulation adopt an explicit and comprehensive definition of illegal content and false information. This should focus on the criminal liability of individuals who produce or disseminate such content or data with the intent to mislead. Such measures would strengthen the protection of European society from the negative impacts of illegal content and false information, ensuring a more robust and harmonised legal framework.

4 THE CRIME OF RECEIVING INCENTIVES TO PUBLISH ILLEGAL CONTENT OR FALSE INFORMATION

Receiving incentives to publish illegal content or false information is a serious offence punishable under national and international laws. In the United Arab Emirates, this crime is regarded as a grave violation of public order and regulations related to combating fraud and defamation, as stipulated in the UAE Anti-Rumours and Cybercrime Law. The increasing use of AI-generated content, including deepfakes and misleading narratives, has further complicated enforcing such laws, especially when financial or ideological motives incentivise such content.[25]

24 European Digital Media Observatory, *Information Disorder and Disinformation Management in Europe: Policy and Practice Overview* (EDMO 2020) < https://edmo.eu/> accessed 25 February 2025.

25 Katarina 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, doi:10.1163/18750230-02901005; Giuseppe Vecchietti, Gajendra Liyanaarachchi and Giampaolo Viglia, 'Managing Deepfakes with Artificial Intelligence: Introducing the Business Privacy Calculus' (2025) 186 Journal of Business Research 115010, doi:10.1016/j.jbusres.2024.115010.

Similarly, the European Union addresses this issue through the Digital Services Act (DSA) and the Code of Practice on Disinformation, focusing on combating false information and illegal content by imposing strict penalties and regulating the responsibilities of digital publishing platforms. However, legal scholars have pointed to the DSA's limited treatment of individual criminal liability, emphasising the need for more robust frameworks to address incentivised disinformation at the individual level.[26]

To thoroughly analyse this crime, this section will explore its elements and the penalties prescribed, comparing the legal framework in the UAE with the provisions of the DSA. This comparison will highlight the similarities and differences between the two systems, shedding light on their respective approaches to addressing this offence.

4.1. The Material Element (Actus Reus)

The material element of the crime of receiving incentives to publish illegal content or false information requires a specific action by the perpetrator. According to Article 55 of the UAE Anti-Rumours and Cybercrime Law, this includes any individual who:

- Requests, accepts or takes any form of benefit.
- Manages or oversees the operation of an abusive account or website.
- Rents or purchases advertising space on such a platform.

This criminal activity involves any benefit obtained by the perpetrator, whether material or non-material or even a promise thereof, in exchange for publishing or republishing illegal content or false information within the UAE using any form of information technology.

The UAE legislator clearly defines the scope of this criminal activity, ensuring that it encompasses all benefits of disseminating harmful or misleading content. Thus, the legislator protects public order and ensures accountability in the digital space.

4.1.1. Forms of Criminal Activity

The first form of criminal activity under examination is the request for illegal content dissemination in exchange for financial incentives**.** This practice involves individuals or entities soliciting the publication of false or unlawful information for monetary gain, thereby contributing to digital misinformation.

The act of requesting involves an individual who owns, manages, or oversees the operation of an electronic account or website initiating a demand for compensation in exchange for publishing or republishing illegal content or false information within the state using information technology. In this scenario, the individual effectively offers the act of

26 Tiernan and Sluiter (n 2).

publication or republication for sale, seeking a promise of compensation without any prior offer from the interested party.

The crime is considered complete upon the request, regardless of whether the request is accepted or rejected by the interested party. Receiving the promised compensation is irrelevant to establishing the crime; the act of requesting alone constitutes a complete offence under the law.[27]

For the crime to materialise, the request must be made by the individual who owns, manages, or supervises the operation of an electronic account or website or through an intermediary. However, in cases involving intermediaries, the request must originate personally from the perpetrator and be conveyed to the interested party through the intermediary.[28]

The request can be made in writing or orally, with no distinction as to the form of communication, as long as the intent and demand are clear.[29]

Another significant form of criminal activity is accepting financial incentives to spread illegal content. In such cases, individuals knowingly agree to distribute false or unlawful information, often leveraging digital platforms to amplify their reach. This behaviour undermines public trust and poses severe legal and ethical implications.

Acceptance occurs when the interested party offers compensation to an individual who owns, manages, or oversees the operation of an electronic account or website to publish or republish illegal content or false information. The crime is considered complete once acceptance occurs, as the meeting of wills between the parties—offer and acceptance—establishes the offence. Significantly, the crime does not depend on the actual implementation of the promised compensation by the interested party; the act of acceptance alone constitutes the offence.[30]

Acceptance does not require a specific form of expression and can be either oral or written, explicit or implicit. Implicit acceptance refers to a legally valid intention where the act of acceptance is inferred from actions that align with the offer. For instance, when the publisher, after becoming aware of the offer, proceeds to publish or republish illegal content in line with the interested party's request, this constitutes implicit acceptance. Determining whether acceptance occurred is a matter for the court of fact, which evaluates the specific circumstances of each case.

27 UAE Cassation Ruling no 354 of 2008 [2009] 1 Collection of Judgments and Legal Principles Issued by the Court of Cassation, Criminal Division, Judicial Year Three, 2009, January 1 to June 30, 114; Vecchietti, Liyanaarachchi and Viglia (n 25).

28 Walid Saad El-Din Mohamed Saeed, 'The Role of Regulatory Bodies and Legislative Measures in Combating Corruption Crimes' (2024) 20(4) The Legal Journal 1489, doi:10.21608/jlaw.2024.354476.

29 Kaur and others (n 1).

30 Osama Hussein Abdel Aal, 'The Crime of Bribery: An Analytical Study' (2017) 59(1) Journal of Legal and Economic Sciences, Ain Shams University 915.

For the crime to be established, acceptance must be serious and genuine. The seriousness of the acceptance reflects the perpetrator's intent and culpability, which are essential elements for imposing criminal liability. If the perpetrator merely pretends to accept the offer to assist authorities in apprehending the interested party in the act, such feigned acceptance negates the offence.[31] Similarly, if the perpetrator lacks a genuine intention to agree with the offer but instead acts to expose the interested party's wrongdoing, the crime of acceptance is not considered established.

The offer from the interested party must also appear serious. Even if the offer lacks genuine intent, its apparent seriousness is sufficient to establish the crime. However, if the offer is blatantly non-serious—such as promising all one's possessions in exchange for publishing illegal content—the crime does not occur. In such cases, any acceptance by the perpetrator does not lead to the establishment of the crime, as the offer lacks the necessary clarity and intent to form a legal agreement.

In this context, a further category of criminal conduct is facilitating monetised disinformation through digital platforms. This occurs when platforms or intermediaries enable the circulation of false information while benefiting financially, whether directly or indirectly. By allowing or failing to regulate such content, these entities play a crucial role in sustaining the economic viability of disinformation campaigns.

This act occurs when the perpetrator receives or benefits from the incentive that constitutes the subject of the crime. This material element is characterised by directly involving the receipt of the incentive, regardless of whether a promise preceded it. Taking is considered the most serious manifestation of the criminal behaviour associated with this offence, as it signifies that the perpetrator has accepted compensation in exchange for publishing or republishing illegal content.[32]

When the perpetrator takes the incentive, the receipt method is irrelevant—it could be physical or symbolic, as long as the act constitutes acceptance of the benefit or advantage related to the crime. Moreover, "taking" includes any form of enjoyment or use of the advantage or benefit provided as part of the offence. This demonstrates the critical nature of this aspect of the crime, as it involves tangible acknowledgement and execution of the illicit agreement.

1.1.1. Forms of Benefits Received by the Perpetrator

The criminal activity in the offence of receiving incentives to publish illegal content or false information—whether through request, acceptance, or taking—must centre around a benefit, incentive, or promise thereof. A benefit or incentive includes anything the

31 Mahmoud Naguib Hosni, *Explanation of the Penal Code: Special Section According to the Latest Legislative Amendments* (6th edn, University Publications House 2019) 321.

32 Al-Anoud Mishaal Al-Ghubayshan Al-Azmi, 'The Crime of Bribery with Case Studies from Reality' (2022) 2(1) Middle East Journal of Legal and Jurisprudential Studies 215.

perpetrator receives, assigns to another, or knowingly agrees to, regardless of its name or type and whether it is material or non-material.

An incentive is anything that fulfils a personal need, no matter how significant or minor that need may be. The most common form of an incentive is money, but it may also be financial documents, securities, jewellery, clothing, food, or any other valuable item. On the other hand, a promise is considered a deferred incentive, carrying the same legal weight as an immediate one.[33]

Incentives can also take the form of services the interested party provides to the publisher or benefits such as facilitating a promotion for an employee, transferring them, lending them an apartment, or granting access to a vehicle for use.[34] Whether the money or benefit comes from a legitimate or illegitimate source is irrelevant.

The incentive itself can also be inherently illegal, such as drugs, stolen property, a bounced check, or a sexual favour in exchange for publishing prohibited content or false information.[35]

The crime is established whether the incentive—in exchange for publishing illegal content or false information—is explicitly apparent or implicitly concealed. For instance, it could involve a formal agreement between the interested party and the publisher, where the latter receives a hidden advantage, such as selling goods at a very low price or purchasing items at an excessively high price.[36]

The law does not require the incentive or benefit to be of substantial value for the crime to be established. The benefit may be large or small, as there is no legal requirement for a proportional relationship between the incentive and the illegal action for which it was offered. The crime is considered complete in either case, as long as the incentive is linked to achieving the purpose of the crime.

However, the crime is not established if the benefit or incentive lacks the intended criminal purpose—such as being a gesture of goodwill, a culturally customary practice, or trivial in value. For example, if the publisher acted out of courtesy or accepted an insignificant and culturally accepted token, the crime does not occur.

33 Abdel Aal (n 30).

34 Saeed (n 28).

35 Nagham Hamad Ali and Ziad Aboud Manajid, 'The Crime of Sexual Bribery' (2022) 33(2) Journal of Al-Maaref University College 93, doi:10.51345/.v33i2.496.g269.

36 Saeed Abdulla Al Nuaimi, Mohammad Amin Alkrisheh and Khawlah M Al-Tkhayneh, 'The Crime of Sexual Harassment: A Comparative Study Between UAE & French Law' (2023) 13(3) Journal of Educational and Social Research 241, doi:10.36941/jesr-2023-0073.

4.1.2. Purpose of the Criminal Act

The purpose of the criminal act in this offence is to publish or republish illegal content or false information within the state using information technology. The crime is contingent upon this specific intent, even if the publisher does not execute the action.

Publishing refers to uploading or sharing content (such as texts, images, videos, or links) on a social media platform or website, making it accessible to others. Publishing can be public (available to all users) or targeted (restricted to specific groups, such as friends or followers). Republishing, however, involves sharing previously published content by another user. For instance, this includes retweeting on X (formerly Twitter), sharing on Facebook, or reposting on other platforms. Republishing often references the source but extends the content's reach to a new audience.

Republishing is legally considered an independent act if it intends to promote or support the original content, especially when it is illegal. Republishing may imply tacit endorsement of the original material unless proven otherwise. It carries the same legal liability as the original publication if the individual republishing the content is aware of its illegality.

From the above, it is clear that UAE law, as outlined in Article 55 of the UAE Anti-Rumours and Cybercrime Law, comprehensively addresses criminal behaviour, including acts of requesting, accepting, and taking incentives. By contrast, European law, as embodied in the Digital Services Act (DSA), does not provide similar provisions criminalising these specific actions, such as requesting, accepting, or taking incentives in exchange for publishing illegal content or false information. Instead, the DSA emphasises the responsibility of digital platforms to manage and remove illegal content when reported.

European law focuses on ensuring compliance with legal obligations related to content moderation and oversight rather than addressing individual motivations behind criminal behaviour.[37] In this framework, the publication or republication of illegal content is deemed a violation if it contravenes transparency and supervision standards. The DSA imposes fines of up to 6% of the platform's global annual revenue for failing to meet obligations related to illegal content. However, it does not extend criminal liability to individuals who receive or accept incentives for publishing such content.[38]

Under the DSA, platforms are required to monitor accounts or sites operating in violation of the law, but direct penalties for individuals managing such accounts in exchange for incentives are absent. This creates a legal loophole concerning criminalising individual actions related to such offences.[39]

37 Regulation (EU) 2022/2065 (n 8) art 3(h).

38 ibid, arts 19, 26, 52.

39 Gail E Crawford and others, *The Digital Services Act: Practical Implications for Online Services and Platforms* (*Latham & Watkins LLP*, 14 March 2023) <https://www.latham.london/2023/03/digital-services-act-practical-implications-for-online-services-and-platforms/> accessed 25 February 2025.

To address this gap, European legislation should incorporate provisions that criminalise the acts of requesting, accepting, or taking incentives for publishing illegal content. Such measures would strengthen European efforts to combat the spread of false information and illicit content by holding individuals accountable for their actions, not just the platforms hosting the content. This approach would bridge the gap in the current regulatory framework, ensuring a more comprehensive and effective legal response to this issue.

4.2. The Mental Element (Mens Rea)

The crime of receiving incentives to publish illegal content or false information is an intentional offence that requires the mental element of criminal intent (*mens rea*). This crime cannot be established through negligence or unintentional acts, as these are not punishable in this context. The perpetrator must possess criminal intent to prove the crime, which comprises two essential elements: knowledge and will.

4.2.1. Knowledge

The perpetrator must be aware of all the legal elements necessary for the crime of receiving incentives to publish illegal content or false information. Specifically, they must know they are requesting, accepting, or taking a benefit in exchange for publishing or republishing illegal content or false information within the state using information technology.

If the perpetrator is unaware that the incentive received is in exchange for publishing or republishing illegal content—such as believing it to be payment for a debt or a gift from a friend on a family occasion unrelated to publication—the criminal intent is absent, and the crime is not established.[40]

Additionally, knowledge of the exchange must exist when receiving the benefit, whether during acceptance or request. Subsequent awareness arising after the act does not constitute the required criminal intent, as post-facto awareness holds no legal relevance in establishing the offence.

4.2.2. Will

The perpetrator's will must be directed toward requesting, accepting, or taking the incentive. The crime is complete even if the perpetrator does not ultimately execute the agreement. For example, the crime occurs if the perpetrator accepts a gift or incentive in exchange for publishing illegal content but later returns the gift or fails to fulfil the agreed-upon act.

40 Chergui Khadija, 'Mechanisms for Monitoring the Crime of Bribery and the Penalties Prescribed for It in Algerian Legislation' (2021) 3(2) Journal of Law and Local Development 58.

The criminal intent required for this crime is classified as general intent, as it only necessitates the perpetrator's intent to fulfil the elements of the crime. There is no requirement for additional intent beyond the act itself.

The burden of proving intent lies with the prosecution, which must establish it through general evidentiary rules. Intent can be demonstrated through any means of evidence. If the perpetrator does not explicitly express their intent in writing or speech, the court may infer it from the circumstances and context of the case.

In contrast, under the Digital Services Act (DSA),[41] UAE law does not address the mental element in detail. The DSA does not explicitly criminalise requesting or accepting incentives in exchange for publishing illegal content or false information. Instead, the European framework focuses on the responsibility of digital platforms to manage and remove illegal content upon being notified.

The DSA prioritises platforms' regulatory obligations over determining individuals' intent or motivations. It emphasises platforms' negligence or failure to monitor or remove illegal content, constituting a regulatory violation. As a result, material actions related to content management, such as reporting and removal, are the primary focus rather than the criminal intent of individual users.[42]

To address this gap, it is recommended that European legislation incorporate provisions that explicitly criminalise the intent and actions of individuals requesting, accepting, or receiving incentives for publishing illegal content. Such an approach would complement existing regulations by ensuring that individuals are held accountable for their actions, strengthening efforts to combat false information and illegal content within the digital ecosystem.

4.3. The Penalty for the Crime

According to Article 55 of the UAE Anti-Rumours and Cybercrime Law,[43] the perpetrator of this crime is punishable by temporary imprisonment and a fine not exceeding AED 2,000,000. The same penalty applies to anyone who manages or supervises the operation of an abusive account or website or rents or purchases advertising space on such platforms. An electronic account or website is considered abusive if it repeatedly publishes false data or content that violates the law.

The UAE legislator has also prescribed two mandatory complementary penalties: proportional fines and confiscation. Article 55 states that "the court shall order the confiscation of the incentive or material benefit obtained, or impose a fine equivalent to its value if it cannot be confiscated." Consequently, the penalty includes temporary

41 Regulation (EU) 2022/2065 (n 8).

42 Crawford and others (n 39); Hoffmann and Gasparotti (n 19).

43 Federal Decree-Law no (34) of 2021 (n 7).

imprisonment ranging from three to fifteen years and a fine between AED 1,000 and AED 2,000,000.[44] The court also orders the confiscation of the incentive accepted by the perpetrator or offered to them. Confiscation applies exclusively to items physically obtained, regardless of whether they are monetary or non-monetary.

Confiscation, a material penalty, is mandatory and cannot be imposed if the criminal act stops at the mere request or acceptance of a promise. In such cases, judges cannot estimate the promise's value or request to impose confiscation. Furthermore, confiscation cannot be applied if the benefit has already been consumed or is non-material.

In cases where the incentive or material benefit cannot be confiscated, the court must impose a fine equal to its value. This proportional fine is mandatory, and the judge cannot waive it. The fine, as specified in the law, is determined according to the specific value of the benefit in each case.

In contrast, European law's Digital Services Act (DSA) does not include explicit provisions criminalising the request, acceptance, or receipt of incentives in exchange for publishing or republishing illegal content or false information. Instead, the DSA focuses on the responsibilities of digital platforms to manage and remove illegal content upon being notified of its presence.

The DSA imposes significant penalties on platforms for non-compliance with their obligations, including fines of up to 6% of their global annual revenue and, in severe cases, suspension or complete prohibition of their services.[45] European legislation indirectly addresses illegal content dissemination by penalising platforms for failing to act rather than focusing on the financial or moral motives of individuals involved in such activities.

While the DSA ensures platform accountability, it does not explicitly address individual behaviours related to incentivised dissemination of illegal content. By contrast, as embodied in Article 55, UAE law explicitly criminalises requesting, accepting, or receiving either material or non-material incentives in exchange for publishing or republishing illegal content. This detailed legislative approach ensures comprehensive coverage of various aspects of the crime and effectively targets its root causes.

To enhance the effectiveness of European efforts in combating the dissemination of false information and illegal content, it is recommended that European legislation adopt a framework similar to UAE law. This should include explicit provisions criminalising the request, acceptance, or receipt of incentives for publishing or republishing illegal content, thereby addressing individual accountability and platform responsibility.

44 As of March 16, 2025, AED 1 equals €0.2501. Therefore, the fines range from approximately €250 (for AED 1,000) to €500,200 (for AED 2,000,000).

45 Crawford and others (n 39); Regulation (EU) 2022/2065 (n 8) art 52.

5 CONCLUSIONS

This study highlights the significance of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes, which provides a comprehensive framework for addressing paid disinformation in the digital world. The UAE legislature has explicitly criminalised various individual behaviours associated with this phenomenon, including requesting, accepting, or receiving incentives in exchange for disseminating illegal content or false information. The law prescribes stringent penalties, including imprisonment, fines, and confiscation, underscoring the state's commitment to maintaining digital and societal security. Beyond criminalising the publication or republication of illegal content, the UAE legal framework also extends to managing and supervising abusive electronic accounts and using advertising spaces for deceptive purposes, further strengthening regulatory oversight.

In contrast, the European Digital Services Act (DSA) primarily focuses on regulating digital platforms and combating illegal content through supervision and removal mechanisms. However, it does not explicitly criminalise individual behaviours related to paid disinformation, leaving a gap in addressing these offences comprehensively. The absence of direct provisions penalising those who request or accept incentives to spread misleading content highlights a significant difference between the UAE and European legal approaches.

Given these findings, several key recommendations emerge. First, the UAE legislature should introduce legal provisions requiring digital platforms to cooperate promptly with legal authorities, ensuring strict enforcement through penalties such as temporary bans or substantial fines for non-compliance. In the European context, the DSA would benefit from explicit legal provisions addressing individual liability for paid disinformation, bridging the existing legal gap and enhancing accountability.

Beyond national legislation, enhancing international cooperation is essential to establishing a unified legal framework for combating paid disinformation crimes. A globally coordinated effort would facilitate consistent definitions and penalties across jurisdictions, strengthening enforcement mechanisms. Additionally, specialised training programs for judges and public prosecutors on the technical and legal aspects of paid disinformation crimes are crucial for ensuring informed judicial and prosecutorial decision-making.

Finally, raising public awareness through national and international education campaigns is necessary to combat the spread of paid disinformation. Encouraging digital responsibility and promoting information verification will play a fundamental role in mitigating the harmful effects of false and misleading content. A multi-faceted approach that combines legal, institutional, and public engagement strategies is essential to addressing the growing challenges posed by paid disinformation in the digital world.

REFERENCES

1. Abdel Aal OH, 'The Crime of Bribery: An Analytical Study' (2017) 59(1) Journal of Legal and Economic Sciences, Ain Shams University 915.
2. Abu Farwa MM, 'Social Media Platforms and Their Legal Liability for Illegal Content' (2022) 39 Kuwait International Law School Journal 161.
3. Al-Azmi AM, 'The Crime of Bribery with Case Studies from Reality' (2022) 2(1) Middle East Journal of Legal and Jurisprudential Studies 215.
4. Ali NH and Manajid ZA, 'The Crime of Sexual Bribery' (2022) 33(2) Journal of Al-Maaref University College 93, doi:10.51345/.v33i2.496.g269.
5. Alkrisheh MA, Al-Katbi SO and Al-Tkhayneh KM, 'The Criminal Confrontation for Crimes of Discrimination and Hate Speech: A Comparative Study' (2024) 7(2) Access to Justice in Eastern Europe 138, doi:10.33327/AJEE-18-7.2-a000210.
6. Al-Mansouri A, 'Publishing and Promoting Fake News between the Criminal Law and the Press and Publishing Law' (2024) 13 Electronic Journal of Legal Research 258 <https://revues.imist.ma/index.php/RERJ/article/view/47387> accessed 25 February 2025.
7. Alneyadi MS and others, 'The Crime of Electronic Blackmail in the Emirati Law' (2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, UAE, November 2022) doi:10.1109/ACIT57182.2022.9994165.
8. Al-Nuaimi SA, Alkrisheh MA and Al-Tkhayneh KM, 'The Crime of Sexual Harassment: A Comparative Study Between UAE & French Law' (2023) 13(3) Journal of Educational and Social Research 241, doi:10.36941/jesr-2023-0073.
9. AL-Tkhayneh KM, Olowoselu A and Alkrisheh MA, 'The Crime in Metaverse (The Future Scenarios for Crime Patterns and the Prospective Legal Challenges)' (2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, UAE, November 2023) doi:10.1109/SNAMS60348.2023.10375402.
10. Crawford GE and others, *The Digital Services Act: Practical Implications for Online Services and Platforms* (*Latham & Watkins LLP*, 14 March 2023) <https://www.latham.london/2023/03/digital-services-act-practical-implications-for-online-services-and-platforms/> accessed 25 February 2025.
11. Hassan HMA, 'Media Publication Crimes: A Comparative Jurisprudential Study with Positive Law – The Crime of Incitement as a Model' (2024) 47 Journal of Jurisprudential and Legal Research 487.
12. Hoffmann A and Gasparotti A, *Liability for Illegal Content Online: Weaknesses of the EU Legal Framework and Possible Plans of the EU Commission to Address them in a "Digital Services Act"* (CEP 2020).
13. Hosni MN, *Explanation of the Penal Code: Special Section According to the Latest Legislative Amendments* (6th edn, University Publications House 2019).

14. Kameel TAR, Kandeel ME and Alkrisheh MA, 'Consumer Protection from Misleading Online Advertisements "An Analytical Study in UAE Law"' (2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, UAE, November 2022) doi:10.1109/ACIT57182.2022.9994108.

15. Kaur A and others, 'Deepfake Video Detection: Challenges and Opportunities' (2024) 57(6) Artificial Intelligence Review 159, doi:10.1007/s10462-024-10810-6.

16. Kertysova K, '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, doi:10.1163/18750230-02901005.

17. Khadija C, 'Mechanisms for Monitoring the Crime of Bribery and the Penalties Prescribed for It in Algerian Legislation' (2021) 3(2) Journal of Law and Local Development 58.

18. Khan I, 'Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (*UN*, 13 April 2021) <https://digitallibrary.un.org/record/3925306?ln=en> accessed 25 February 2025.

19. Mohamed AAR, 'Civil Responsibility For Providers Of Illicit Content Circulating On The Internet (A Comparative Study Between French Law And Egyptian Law)' (2020) 35(3) Journal of the Faculty of Sharia and Law, Tanta University 1074, doi:10.21608/mksq.2020.111506.

20. Mohammed AGH, 'Mechanisms of the Egyptian Public in Verifying Fake News and its Relationship their Interactive Patterns on Social Networking Sites' (2021) 59(2) Journal of Media Research 1003, doi:10.21608/jsb.2021.199620.

21. Raman R and others, 'Fake News Research Trends, Linkages to Generative Artificial Intelligence and Sustainable Development Goals' (2024) 10(3) Heliyon e24727, doi:10.1016/j.heliyon.2024.e24727.

22. Saeed WS, 'The Role of Regulatory Bodies and Legislative Measures in Combating Corruption Crimes' (2024) 20(4) The Legal Journal 1489, doi:10.21608/jlaw.2024.354476.

23. Tiernan M and Sluiter G, 'The European Union's Digital Services Act and Secondary Criminal Liability for Online Platform Providers: A Missed Opportunity for Fair Criminal Accountability?' (*SSRN*, 18 March 2024) doi:10.2139/ssrn.4731220.

24. Vecchietti G, Liyanaarachchi G and Viglia G, 'Managing Deepfakes with Artificial Intelligence: Introducing the Business Privacy Calculus' (2025) 186 Journal of Business Research 115010, doi:10.1016/j.jbusres.2024.115010.

25. Yar M, 'A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media' (2018) 1(1) International Journal of Cybersecurity Intelligence & Cybercrime 5, doi:10.52306/01010318RVZE9940.

AUTHORS INFORMATION

Mohammad Amin Alkrisheh*
Dr.Sc. (Law), Full Professor, College of Law, Al Ain University, Al Ain, United Arab Emirates
mohammad.alkrisheh@aau.ac.ae
https://orcid.org/0000-0002-3649-9494
Corresponding author, responsible for research methodology, data collection, writing, and supervising. Writing – original draft, Writing – review & editing and supervising

Fatiha Mohammed Gourari
Dr.Sc. (Law), Full Professor, Dean of the College of Law, United Arab Emirates University, Al Ain, United Arab Emirates
fgourari@uaeu.ac.ae
https://orcid.org/0009-0002-2458-9502
Co-author, responsible for research methodology, data collection, writing, and supervising. Writing – original draft, Writing – review & editing and supervising

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

ABOUT THIS ARTICLE

Cite this article
Alkrisheh MA and Gourari FM, 'Criminal Liability For Paid Disinformation In The Digital World: A Comparative Study Between UAE Law And The European Digital Services Act (DSA)' (2025) 8(2) Access to Justice in Eastern Europe 341-64 <https://doi.org/10.33327/AJEE-18-8.2-r000110>

DOI https://doi.org/10.33327/AJEE-18-8.2-r000110

Managing Editor – Mag. Yuliia Hartman. **English Editor** – Julie Bold.
Ukrainian Language Editor – Liliia Hartman.

Keywords: *paid misinformation, false information, criminal liability, cybercrimes, UAE law, European Digital Services Act (DSA), digital platforms, deepfake, AI, rumours.*

DETAILS FOR PUBLICATION

Date of submission: 15 Mar 2025
Date of acceptance: 08 Apr 2025
Date of publication: 14 May 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round, revised version submitted 06 Apr 2025

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Оглядова стаття

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ОПЛАЧЕНУ ДЕЗІНФОРМАЦІЮ У ЦИФРОВОМУ СВІТІ: ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ ЗАКОНОДАВСТВА ОАЕ ТА ЗАКОНУ ЄС ПРО ЦИФРОВІ ПОСЛУГИ (DSA)

Могаммад Амін Алкрішег* і Фатіха Могаммед Ґурарі

АНОТАЦІЯ

Вступ. *Завдяки швидкій цифровій трансформації та широкому використанню платформ соціальних медіа розповсюдження різних форм шкідливого цифрового контенту, включно з незаконним контентом і неправдивою чи оманливою інформацією, особливо коли це фінансово стимулюється, стало актуальною глобальною проблемою. Такі практики загрожують цифровій довірі та створюють значні ризики для суспільної стабільності. Незважаючи на посилення правових зусиль щодо боротьби з цими злочинами, єдиної та*

комплексної законодавчої бази все ще бракує. У цьому дослідженні розглядається кримінальна відповідальність, пов'язана з оплаченою дезінформацією в цифровому світі, здійснено порівняння правового підходу, що передбачений законодавством ОАЕ та Законом ЄС про цифрові послуги (DSA). У той час як ОАЕ прийняли спеціальні положення, спрямовані на монетизацію дезінформації, європейське законодавство зосереджене насамперед на обов'язках цифрових платформ без прямого звернення до окремих учасників, залучених до такої діяльності.

Методи. *У статті використовується порівняльно-правовий аналіз, увагу зосереджено на відповідних законодавчих положеннях в обох юрисдикціях. У дослідженні застосовано аналітичний і порівняльний підхід для вивчення статті 55 Закону ОАЕ про боротьбу з плітками та кіберзлочинністю, яка чітко криміналізує фінансові стимули для поширення незаконного контенту. Також було здійснено оцінку Європейського DSA, який в основному регулює підзвітність платформи, але не містить прямих положень про індивідуальну кримінальну відповідальність за оплачену дезінформацію. Аналіз охоплює доктринальні юридичні та тематичні дослідження, щоб підкреслити ефективність і обмеження кожної правової системи в боротьбі з цією проблемою.*

Результати та висновки. *Дослідження виявило, що законодавство ОАЕ забезпечує більш структуровану та детальну правову базу для боротьби з платною дезінформацією, пропонуючи чіткі кримінальні санкції для осіб, причетних до таких дій. Європейський DSA, навпаки, використовує ширший регуляторний підхід, зосереджуючись на інституційному нагляді, не розглядаючи безпосередньо кримінальну відповідальність осіб, причетних до монетизованої дезінформації. У дослідженні рекомендується, щоб європейське законодавство прийняло більш конкретну модель боротьби з цими злочинами, інтегрувавши пряму кримінальну відповідальність поряд із регулюванням платформ. Крім того, у статті наголошено на необхідності посилення міжнародного співробітництва та гармонізації регулювання для того, щоб посилити цифрову прозорість та зменшити ризики, пов'язані із фінансово мотивованою дезінформацією.*

Ключові слова: *оплачена дезінформація, неправдива інформація, кримінальна відповідальність, кіберзлочини, законодавство ОАЕ, Закон ЄС про цифрові послуги (DSA), цифрові платформи, діпфейк, AI, плітки.*