DOI https://doi.org/10.30525/978-9934-26-686-7-8

CRIMINAL PROCEDURAL AND FORENSIC ASPECTS OF PROVING HATE SPEECH IN THE DIGITAL ENVIRONMENT

Koval A. A., Kazarian E. H.

INTRODUCTION

Countering hate speech on the Internet, social media platforms, and within the public sphere constitutes one of the central challenges facing contemporary democratic societies and represents an important dimension of the implementation of the 2030 Agenda for Sustainable Development. Hate speech undermines the fundamental values of the European Union (EU) – respect for human dignity, equality, freedom, democracy, and the rule of law – and poses a serious threat to human rights, social cohesion, and public security. For Ukraine, which is confronting full-scale armed aggression while simultaneously pursuing a strategic course toward European integration, the issue of hate speech has acquired particular urgency. The escalation of social tensions, the systematic dissemination of disinformation, and the active exploitation of digital platforms as instruments of information warfare contribute to the normalization of hatred and discrimination, thereby directly endangering human rights, societal resilience, and democratic stability.

Hate speech should be regarded not merely as a socio-communicative phenomenon but, above all, as a human rights concern requiring clear and effective legal mechanisms of response. In this regard, European standards developed within the framework of EU law and the Council of Europe play a pivotal role, including the case law of the European Court of Human Rights, recommendations of the Committee of Ministers of the Council of Europe, the work of the European Commission against Racism and Intolerance, and the EU Code of Conduct on Countering Illegal Hate Speech Online.

According to data from the Office of the Prosecutor General of Ukraine, the number of criminal offences recorded under Article 161 of the Criminal Code of Ukraine between 2019 and 2025 has remained consistently high, ranging from 65 to 123 cases annually [1]. The overall trend indicates the persistent and systemic nature of the problem, particularly given the significant latency of such offences.

Accordingly, the detection and investigation of hate speech in the digital environment, especially on social media platforms, remains an issue of exceptional relevance. It is directly linked to the protection of human rights, the safeguarding of information security, the preservation of social harmony, and the effective functioning of democratic institutions in the face of emerging global challenges.

[1] Офіс Генерального прокурора. Офіційний сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

1. Theoretical and Legal Foundations for Countering Hate Speech

In pursuing its European integration trajectory, Ukraine has undertaken commitments to comply with international standards on equality and non-discrimination, including the Convention for the Protection of Human Rights and Fundamental Freedoms [2], the Council of Europe Framework Convention for the Protection of National Minorities, Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech[3], and Recommendation No. R (97) 20 on "hate speech"[4].

Despite these commitments, the use of hateful rhetoric and incitement to hostility continues to proliferate. According to data from the National Police of Ukraine and civil society monitoring organizations, more than 370 instances of public dissemination of hate speech on social media were recorded in 2024 alone. Approximately 70% of these cases involved discrimination on the grounds of nationality, religion, or sexual orientation [5].

Hate speech encompasses calls for discrimination, the promotion of the superiority of one group over another, dehumanization, and the dissemination of hostile or degrading imagery [6]. Its regulation inevitably requires a careful delineation between the constitutionally protected right to freedom of expression and the obligation to safeguard the rights and dignity of vulnerable groups. At the same time, it is worth emphasizing that in everyday communication a significant part of society does not realize that it uses elements of hate speech with regard to certain groups, considering such expressions socially acceptable (for example, "Asians," "Caucasians," etc.)[7].

Criminal liability for hate speech-related offences in Ukraine is governed, inter alia, by Article 161 of the Criminal Code – violation of citizens' equality, Article 300 – distribution of works promoting violence and cruelty, Articles 109 and 110 – public calls for violent change of government and encroachment upon territorial integrity, Article 436 – propaganda of war (in cases where hate speech takes the form of advocating armed aggression or inciting armed conflict), and Article 436-1 – production and dissemination of communist and National Socialist (Nazi) symbols

[2] Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 4 https://zakon.rada.gov.ua/laws/show/995004#Text.

[3] Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech. *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: https://search.coe.int/cm?i=0900001680a67955.

[4] Рекомендація № R (97) 20 Комітету Міністрів державам-членам щодо «мови ненависті». *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech" – Freedom of Expression.

[5] Національна поліція України. Офіційний сайт. URL: https://npu.gov.ua/.

[6] Коваль А. А. Толерантність онлайн: проблеми дотримання прав людини в соціальних мережах та правові шляхи їх вирішення. *Національні інтереси України*. № 5 (10). 2025. С. 616. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-609-619.

[7] Казарян Е. Г. Поняття та особливості мови ворожнечі. *Х Юридичні могилянські читання – 2024 :* матеріали Х всеукраїнської наук.-практ. конф. (м. Миколаїв, 28 квіт. 2024 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2024. С. 23. URL: https://chmnu.edu.ua/wp-content/uploads/Mogilyanski_chitannya_-_2024.pdf.

and propaganda of totalitarian regimes (applicable where hate speech is associated with the glorification of such regimes or the promotion of their ideologies) [8].

Preventing and countering hate speech and incitement to hatred on the Internet, particularly on social media platforms, is inherently complex and multidimensional. A central component of this process is evidentiary activity in criminal proceedings of this category, aimed at ensuring the criminal accountability of perpetrators.

The digital nature of offences related to incitement to hatred and discrimination on social media entails a number of specific features.

First, particular attention must be paid to the detection and preservation of digital traces containing information about the dissemination or incitement of hatred. In addition to complaints submitted by victims, law enforcement authorities conduct proactive monitoring of open sources through specialized cybersecurity units across platforms such as Facebook, X (Twitter), Telegram, TikTok, YouTube, and Instagram. Since the servers of social media platforms are often located outside Ukraine, timely access to relevant data may be complicated. Accordingly, it is essential to employ international legal assistance mechanisms (MLAT requests, Interpol channels) and cooperation frameworks with digital platforms (for example, Facebook Transparency Center).

Currently, both European states and Ukraine utilize specialized digital forensic tools to detect and analyze hate speech in social media. These include data extraction and forensic analysis software such as FTK (Forensic Toolkit), EnCase, and X-Ways Forensics, which are applied to examine storage devices and recover deleted files. Tools such as Cellebrite and Oxygen Forensics are widely used in the examination of mobile devices, enabling the analysis of text messages, call records, and geolocation data.

Network traffic analysis is conducted using Wireshark, while Maltego enables the collection of OSINT data and the mapping of relationships between individuals. Big data analytics technologies, such as Splunk and the ELK Stack, are applied to process large volumes of information and identify behavioral patterns among users. Data decryption tools, including Passware Kit and Elcomsoft, facilitate the recovery of encrypted files and electronic communications[9].

According to international practice, key digital forensic instruments used in the analysis of social media include the following:

1. Pipl – a service that aggregates data from online archives based on a single variable (such as an email address or phone number) and provides access to additional relevant personal information [10].

---

[8] Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[9] Казарян Е. Г. Роль засобів цифрової криміналістики у розпізнаванні мови ворожнечі у соціальних мережах. *XI Юридичні могилянські читання – 2025* : матеріали XI всеукраїнської наук.-практ. конф. (м. Миколаїв, 24 квіт. 2025 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2025. С. 60–61. URL: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2794/1/XI%20Юридичні%20Могилянські%20читання.pdf.

[10] Ziwen T., Channing Z. China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy.* 2021. Vol. 5 (1). Pp. 7–25. DOI: https://doi.org/10.69554/NATU8989.

2. WebPreserver – an automated web and social media archiving tool capable of rapidly collecting online content, expanding hidden replies and comments, and preserving social media profiles from multiple platforms [11].

3. Makeawebsitehub – a resource that regularly updates listings of emerging social interaction applications, which may assist investigators in expanding web-based inquiries and identifying lesser-known platforms potentially containing relevant information [12].

4. TinEye – a reverse image search tool that enables identification of original images and detection of other websites where the same image has been used, thereby assisting in tracing the source of visual content shared on social media[13].

5. TweetBeaver – a tool designed to extract substantial volumes of data from public Twitter (X) accounts and to analyze connections between accounts[14].

Empirical research conducted by foreign scholars indicates that the BiLSTM (Bidirectional Long Short-Term Memory) model demonstrates high accuracy in detecting hate speech. Owing to its enhanced sensitivity to contextual and semantic features, as well as sequential patterns in textual data such as tweets, BiLSTM proves particularly effective in identifying the complex and nuanced manifestations of hate speech[15].

Upon detecting publications, comments, videos, or images that may contain elements of hate speech, the content must be properly preserved by creating screenshots, screen recordings, and saving relevant metadata (URL address, date and time of publication, account identifiers, IP address, hashtags, etc.).

Within the framework of contemporary approaches to criminal investigations, digital forensic tools are acquiring increasing significance in both international and national practice. Their application facilitates the detection, preservation, and substantiation of criminal conduct, thereby contributing to the effective implementation of the principle of inevitability of punishment. Scholarly literature emphasizes the importance of an integrated use of the following instruments:

– keyword- and hashtag-based search mechanisms, with lists developed in accordance with thematic or regional focus;

---

[11] Thouvenin F., Hettich P., Burkert H., Gasser U. 4 web archives. In: Remembering and Forgetting in the Digital Age. *Law, Governance and Technology Series.* 2018. Vol. 38. Springer, Cham. Pp. 84–101. DOI: https://doi.org/10.1007/978-3-319-90230-2_6.

[12] Spencer J. 101 social networking sites you need to know about in 2022. 2021. URL: https://makeawebsitehub.com/social-media-sites/.

[13] Kondal M., Singh, V. Comparative analysis of tineye and google reverse image search engines. *International Journal of Innovative Science and Research Technology.* 2022. Vol. 7 (1). Pp. 205–207. DOI: https://doi.org/10.5281/zenodo.6378256.

[14] Lyndon R., Tse V., Moore L., May-Hobbs M. Disinformation in Brazil: The 2019 Amazon fires on social media. In: Mair M., Meckin R., Elliot M. (Eds) *Investigative Methods: An NCRM Innovation Collection.* Southampton: National Centre for Research Methods. 2022. Pp. 44–53. DOI: https://doi.org/10.5258/NCRM/NCRM.00004547.

[15] Toktarova A., Syrlybay D., Myrzakhmetova B., Anuarbekova G., Rakhimbayeva G., Zhylanbaeva B., Suieuova N., Kerimbekov M. Hate Speech Detection in Social Networks using Machine Learning and Deep Learning Methods. *International Journal of Advanced Computer Science and Applications.* 2023. Vol. 14 (5). P. 396. DOI: https://doi.org/10.14569/IJACSA.2023.0140542.

– Big Data technologies for identifying patterns and visualizing information flows;

– analysis of geolocation data, as well as photo and video materials obtained from open sources and digital platforms;

– application of image and video processing software to detect falsifications or confirm authenticity;

– examination of data extracted from electronic devices, including stored files, messages, and call records;

– identification of users and objects through facial recognition systems combined with database cross-referencing.

Although technologically sophisticated, these instruments substantially expand the possibilities of digital evidentiary practice, including in criminal proceedings related to hate speech offences [16].

Among the current directions of digital forensic research, the following may also be distinguished:

– analysis of data stored in cloud environments, including the identification, extraction, and authentication of information located on remote servers;

– examination of mobile devices, primarily smartphones, aimed at establishing data structure, communication history, deleted objects, and other relevant artifacts;

– analysis of information exchange applications (messengers, social networks, encryption software) used on mobile devices and computers;

– investigation of Internet of Things (IoT) devices – network-connected "smart" devices such as surveillance cameras, trackers, and sensors;

– network forensics, involving the analysis of traffic structure, access logs, IP addresses, and other digital traces within network environments;

– examination of modern interactive devices and virtual assistants (including Amazon Alexa, Google Assistant, Siri) capable of storing voice command records and user activity logs;

– analysis of non-standard data sources not directly related to smartphones, such as local and online databases, instant messaging systems (e.g., AOL IM), operational memory (including volatile memory), segments of the Darknet, anti-forensic tools, deleted or fragmented files, flash drives, cryptocurrencies, and related artifacts;

– digital behavioral analysis of individuals or groups, enabling reconstruction of activity patterns, interactions, social connections, and communication models;

– digital forensic intelligence, including OSINT (open-source intelligence), used to detect threats, verify facts, and identify offenders within the open information environment[17].

Taken together, these areas demonstrate the integrated nature of digital forensics as a field combining legal, technical, linguistic, and social analytical approaches necessary for the effective investigation of crimes committed in the digital environment, including those related to hate speech.

---

[16] Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika:* XVIII. 2022. Т. 18. С. 32.

[17] Reedy P. Interpol review of digitalevidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520. DOI: https://doi.org/10.1016/j.fsisyn.2020.01.015.

Secondly, a distinct stage of proof involves the technical identification of the perpetrator and the establishment of a hate motive. Given the possibility of using anonymous accounts or VPN services, investigators must obtain data from service providers (including IP addresses and connection timestamps), as well as establish a link between a specific account and an identified individual through log files, mobile devices, email accounts, and other digital traces. It is equally essential to ensure the proper preservation of digital evidence: screenshots must be duly documented and certified, with accurate recording of the URL, date, and time of capture.

Particular complexity arises in establishing and proving the motive of hatred, which constitutes a mandatory element of the corpus delicti in relevant criminal offences. It is not sufficient merely to document the dissemination of offensive or inciting statements; it must also be demonstrated that the act was committed specifically out of hatred based on race, nationality, gender, language, religion, sexual orientation, or other protected characteristics. This requires thorough contextual analysis of publications, assessment of the frequency and direction of hostile expressions, and examination of the individual's profile, including preferences, subscriptions, and prior statements.

For criminal liability to arise under the relevant provisions of the Criminal Code of Ukraine, proof of a hate motive is indispensable. This presents challenges for investigators due to the delicate boundary between constitutionally protected freedom of expression and unlawful manifestations of intolerance. In this regard, investigators and judges should take into account the jurisprudence of the European Court of Human Rights (ECtHR), which clearly distinguishes "protected freedom of expression" from "hate speech" that falls outside the scope of protection.

In its case law, the ECtHR has repeatedly emphasized that freedom of expression is not absolute and does not extend to statements that promote hatred, violence, or the dehumanization of individuals based on race, nationality, religion, or other identity characteristics. In particular, in Norwood v. the United Kingdom (2004), the Court declared the applicant's complaint inadmissible. In that case, Mark Anthony Norwood, a member of the British National Party, displayed a poster in his window depicting the burning Twin Towers accompanied by a slogan calling for the expulsion of Islam. The Court held that such conduct was incompatible with the values of the Convention and fell within the scope of Article 17 (prohibition of abuse of rights). The decision underscored that public statements amounting to a general attack on a religious group and inciting hatred are not protected under Article 10 of the Convention, even in the absence of explicit calls for violence. The Court concluded that Norwood's actions constituted an attack on the values of tolerance and non-discrimination [18].

The ECtHR has consistently held that even in the absence of explicit calls for physical violence, statements may qualify as hate speech if they create an atmosphere of intolerance or justify discrimination. In Vejdeland and Others v. Sweden (2012), the Court found no violation of Article 10 of the Convention. The applicants had

[18] Case of Norwood v. the United Kingdom (Applications no. 23131/03): Judgment European Court of Human Rights, 16 November 2004. URL: https://hudoc.echr.coe.int/eng?i=001-67632.

been convicted for distributing homophobic leaflets in students' lockers at a secondary school. Although they argued that their intention was to initiate debate about educational objectivity, the Court considered the content of the leaflets excessively offensive, as homosexuality was described as a "sexual deviation," alleged to have a "morally destructive effect" on society, and falsely associated with the spread of HIV/AIDS and the minimization of pedophilia. The Court emphasized that, even without direct incitement to violence, such allegations were serious and prejudicial. Particular weight was given to the method of distribution–directly targeting schoolchildren, a vulnerable audience, within a school to which the applicants had no lawful access. The sanctions imposed were deemed proportionate and necessary in a democratic society for the protection of the rights of others[19].

The ECtHR further underscores that the decisive factor in assessing alleged hate speech is context, including the socio-political climate, the role of the speaker, and the nature of the intended audience. Thus, in Perinçek v. Switzerland, on 15 October 2015, the ECtHR found a violation of Article 10 of the European Convention on Human Rights concerning freedom of expression.

The applicant, Doğu Perinçek, had publicly described the events of 1915 concerning the Armenians as an "international lie" and was subsequently convicted in Switzerland. While the Court acknowledged that the conviction constituted interference prescribed by law and pursuing a legitimate aim, it concluded that the restriction was not necessary in a democratic society. The statements concerned a matter of public interest, did not amount to incitement to hatred or violence, and were made in a context not characterized by heightened social tension. The penalty was considered disproportionate, and the Court noted the absence of an international obligation requiring Switzerland to criminalize such statements. On these grounds, the ECtHR established a violation of Article 10 of the Convention[20].

The ECtHR further recognizes that hate speech may manifest not only in verbal but also in symbolic forms, including posters, images, metaphors, and ironic constructions. In 2000, a book by Guillaume Faye entitled La Colonisation de l'Europe: Discours vrai sur l'immigration et l'Islam was published in France. The author asserted that Europe was gradually being "colonized" by Muslims, allegedly leading to an ethnic civil war, which he portrayed as a necessary "solution". The text employed expressions such as "ritual rapes" and "territorial partisans". French courts found the author and publishers guilty of incitement to hatred, discrimination, or violence on grounds of origin, race, or religion, imposing fines. The ECtHR held that there had been no violation of Article 10 (freedom of expression). It emphasized that numerous passages in the book portrayed entire communities in a negative light and were capable of arousing feelings of hostility and rejection among readers. The interference was prescribed by law and pursued the legitimate aim of protecting public order and the rights of others. Although the French Government relied on Article 17 of the Convention (prohibition of abuse of rights), the Court opted to assess the case under Article 10, concluding that while the content was inflammatory,

[19] Case of Vejdeland and others v. Sweden (Applications no. 1813/07): Judgment European Court of Human Rights, 9 February 2012. URL: https://hudoc.echr.coe.int/fre?i=001-109046.

[20] Case of Perinçek v. Switzerland (Applications no. 27510/08): Judgment European Court of Human Rights, 15 October 2015. URL: https://hudoc.echr.coe.int/eng?i=001-158235.

it did not reach the threshold required for the complete exclusion of Convention protection[21].

Thirdly, it must be emphasized that in criminal proceedings concerning incitement to hatred, discrimination, or calls to violence on social media, the application of specialized knowledge and expert examinations is pivotal for the correct legal qualification of the act and for substantiating suspicion or indictment.

2. Specific Features of Proving Hate Speech in the Digital Environment

Given the multi-layered nature of digital offences, cases involving hate speech frequently require complex forensic examinations encompassing several fields of expertise: linguistic (semantic and textual) analysis to identify elements of hate speech and incitement to violence; psychological assessment to evaluate the impact of content on the emotional and volitional sphere of recipients; authorship attribution to determine the authorship of disputed texts or images; and computer-technical examination to analyze metadata, IP addresses, timestamps, and sources of upload.

The quality of expert findings largely depends on the precision and correctness of the questions posed. Typical inquiries include: Does the text contain elements of incitement to racial, national, or religious hatred? Are the statements aimed at degrading the dignity of a specific social group? Do the expressions constitute a call for discrimination? Can the disputed post or comment be attributed to a particular individual? Improperly formulated questions may result in inconclusive opinions or necessitate repeated examinations.

For submission of materials for expert analysis, digital evidence must be properly secured and documented, including electronic storage devices, certified copies of web pages, and log extracts. The contextual framework of publication – date, time, platform, user reactions – must be recorded, and a technical specialist or forensic investigator should verify the authenticity and integrity of the data.

In examining linguistic content potentially containing unlawful elements, it is essential to rely on forensic linguistic expertise grounded in philological methodology, particularly linguistics. Specialized linguistic knowledge enables in-depth analysis of texts to determine the existence of speech-related delicts, their communicative orientation and function within a specific context, and, where necessary, the likely author – especially in cases involving anonymous or extremist communications.

Forensic linguistic examination constitutes a specialized scientific analysis of a text or other speech product conducted to answer legally relevant questions. Spoken or written words may, in certain circumstances, acquire legal significance and be treated as actions entailing legal consequences.

The object of such examination is the text as part of a broader discourse, within which communicative norms operating in a particular social or informational

[21] Case of Soulas and others v. France (Applications no. 15948/03): Judgment European Court of Human Rights, 10 October 2008. URL: https://globalfreedomofexpression.columbia.edu/cases/soulas-and-others-v-france/.

environment are assessed. Deviations from these norms may be interpreted as unlawful conduct[22].

Procedurally, forensic linguistic analysis encompasses both formal linguistic structures and semantic content. Its purpose is to identify lexical constructions, stylistic devices, and semantic units that may indicate unlawful expression under specific provisions of criminal or administrative law[23].

In the context of the growing prevalence of information-related offences, particularly in digital environments, linguistic expertise has evolved from an occasional evidentiary tool into a systemic component of forensic practice. This is especially relevant in criminal proceedings involving hate speech, incitement to violence, discrimination, or threats, where a proper legal assessment of textual evidence is impossible without specialized philological knowledge[24].

Within the framework of this research topic, it is appropriate to outline the specific features of expert analysis of linguistic content. Lexical analysis is aimed at identifying words and phrases that carry negative, degrading, derogatory, or aggressive semantics directed at an individual or a group defined by particular characteristics (national, ethnic, religious, social, etc.).

Attention is paid to direct insults and invective language, dehumanizing designations (such as comparisons with animals, objects, or diseases), as well as lexical units calling for exclusion, destruction, or restriction of rights. A statement such as “these [derogatory term] have no right to live among us” contains negatively marked vocabulary and constructs an exclusionary narrative aimed at removing a particular group from the social space.

Syntactic constructions. At the syntactic level, expert examination focuses on identifying forms of linguistic influence, particularly constructions of an imperative or exhortative nature that encourage action or contain explicit or implicit calls to aggression. Special consideration is given to the imperative mood of verbs, rhetorically manipulative questions, and conditional constructions that may justify violence. For example, a phrase such as “the city must be cleansed of them,” while not explicitly calling for violence, demonstrates an imperative orientation and may be interpreted as encouraging hostile action.

Stylistic devices. Linguistic expert examination also encompasses indirect forms of hostility that may be disguised as humor, irony, or artistic expression. The analysis focuses on sarcasm and irony that undermine dignity, hyperbole intensifying negative portrayals, as well as allusions and metaphors understandable to a particular audience. For instance, the statement “they are, as always, ‘extremely useful’ to

[22] Ажнюк Л. В. Лінгвістична експертиза як юридичний інструмент. *Магістеріум. Мовознавчі студії*. 2017. Вип. 66. С. 14.

[23] Коваль А. А. Петренко К. Д. Мова ворожнечі у цифровому просторі: особливості розслідування. *Вісник ЛННІ ім. Дідоренко*. 2025. Вип 3 (111). С. 97. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/80. DOI: https://doi.org/10.32782/2786-9156.111.3.

[24] Черняк А. М. Використання спеціальних знань при дослідженні текстів, із закликами до підриву конституційного ладу, порушення територіальної цілісності і недоторканості України. *Вісник кримінального судочинства*. 2023. № 3–4. С. 106. DOI: https://doi.org/10.17721/2413-5372.2022.3-4/101-111.

society," when used in a negative discussion context, may carry a sarcastic connotation and convey contempt without explicit insult.

Context of expression. Contextual analysis is crucial for the accurate interpretation of a statement, as the meaning of particular phrases may substantially change depending on their communicative environment. Experts take into account the author's preceding and subsequent publications, the general theme of the page or channel, audience reactions (comments, shares), and the broader socio-political or informational background. The same phrase may be neutral within an academic debate but acquire characteristics of hate speech if systematically employed in a series of publications targeting a specific social group [25].

Thus, linguistic examination of hate speech is inherently comprehensive in nature and is based on the combined application of lexical, syntactic, stylistic, and contextual analysis. It is precisely the cumulative assessment of these elements that enables a well-reasoned conclusion as to the presence or absence of hate speech indicators in specific digital content.

Moreover, in the context of the development of the information society, the examination of digital traces acquires particular significance in the investigation of hate speech-related offences, as such traces may indicate the presence of a specific motive – intolerance. Taking into account contemporary scientific approaches to determining the necessity of forensic examinations in cases of this category, special emphasis should be placed on the conduct of information and computer forensic examination (ICFE). This type of examination constitutes a subtype of computer-technical expertise within the broader category of engineering and technical forensic examinations. ICFE ensures the identification, preservation, analysis, and safeguarding of digital evidence that might otherwise remain inaccessible.

Through the application of modern technologies, it becomes possible to analyze data obtained from computer devices, mobile phones, cloud services, and social media platforms. This is particularly relevant given that offenders increasingly rely on digital technologies to plan, coordinate, and disseminate unlawful activities, thereby complicating the use of traditional investigative methods. In such circumstances, ICFE often represents the only effective means of obtaining reliable and admissible information [26].

ICFE is aimed at establishing circumstances related to the creation, processing, and storage of information on computer systems and digital media. Its primary task consists in the search, identification, reconstruction, and technical analysis of data generated either by a user or by software within a computer system [27]. For this purpose, experts are provided with various objects of examination, including personal computers, mobile

[25] Ажнюк Л., Ажнюк Б. Семантико-текстуальна лінгвістична експертиза усного й писемного мовлення: науково-методичні рекомендації. Київ, 2022. 47 с.

[26] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 47. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

[27] Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Istoryko-pravovyi chasopys.* 2017. № 1 (9). С. 141.

phones, tablets, data storage devices (hard drives, flash drives), and other electronic devices that may contain traces of criminal activity. The expert may determine whether the submitted object contains information in any form – files, audio, video, correspondence, social media posts–relevant to establishing indicators of a hate motive. Additionally, the expert may assess whether the examined device contains deleted files (graphic, textual, video, audio) and whether such data can be recovered[28].

ICFE is conducted to identify, preserve, and analyze data from digital media that may confirm the preparation or commission of a criminal offence. It plays a pivotal role in the investigation of crimes motivated by intolerance, as it enables the identification of a specific motive through the examination of informational content, electronic correspondence, and communications on social media platforms.

Within the framework of ICFE, specialists analyze computer equipment, mobile devices, and digital storage media in order to detect files containing extremist content indicators, as well as to examine correspondence, browser history, messengers (such as WhatsApp or Telegram), and other sources of digital evidence. The particular features of this examination stem from the need not only to establish the fact of unlawful conduct but also to identify a specific hate motive, uncover organized criminal networks, analyze propaganda materials, and overcome technical barriers associated with modern data encryption methods [29].

Where computer data stored in electronic devices have been created or modified as a result of actions undertaken by an offender or other persons during or in connection with the commission of a criminal offence, such data acquire evidentiary value. They may be seized and analyzed as electronic (digital) traces of the offence. In this context, electronic (digital) traces should be understood as computer information that has arisen or been modified through user interaction with computer systems in connection with criminal activity[30].

One of the principal objectives of ICFE is the identification of a motive of intolerance. In many instances, perpetrators leave digital traces reflecting deliberate actions carried out in the virtual environment aimed at forming, developing, or implementing an ideological, informational, or organizational foundation for committing a violent crime motivated by hostility toward a particular group defined by race, ethnic origin, religion, or worldview. Such traces may include video recordings, textual documents, social media correspondence, or messenger communications containing hostile statements or direct threats against specific social, ethnic, or religious groups. The analysis of such materials makes it possible

[28] Kazarian E. The use of special knowledge in the investigation of murders motivated by racial, national or religious intolerance. *Věda a perspektivy*. 2023. № 12 (31). P. 268–269. DOI: https://doi.org/10.52058/2695-1592-2023-12(31)-260-271.

[29] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 48. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

[30] Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2022. № 4 (100). С. 230. DOI: https://doi.org/10.33766/2524-0323.100.226-236.

to establish a link between the suspect and the ideological platform that inspired or motivated the commission of the offence.

Particular attention during ICFE is paid to digital evidence related to the consumption, dissemination, and interaction of a user with extremist content. Such content may be distributed in open or semi-closed environments, including social media platforms, specialized Telegram channels, Discord servers, forums, or platforms such as Reddit. This may involve viewing videos containing violent or propagandistic narratives, reading and storing texts, memes, manifestos, or similar materials. Typical digital traces of such activity include search history, browser cache, subscription lists, "likes," visited resources, and downloaded files. The identification of these traces enables investigators to reconstruct stages of an individual's ideological transformation – from initial exposure to radical content to the internalization and potential implementation of hostile attitudes through violent actions.

Electronic traces are of particular value in the investigation of serious crimes, including intentional homicide, even where such traces are not directly connected to the moment of the offence. Digital data may contribute to establishing the subjective element of the crime, including motives, purposes, psychological characteristics of the offender, and, in some cases, location data. Of special importance is the analysis of information capable of demonstrating whether the offence was committed on grounds of intolerance. Such information may be reflected in social media posts, correspondence, comments, or publications made before or after the offence[31].

Digital traces stored on remote information carriers and available in open Internet sources – for example, on social media platforms or forums containing extremist content – may be identified and preserved using standard computer tools, including personal computers and web browsers. Methods of documentation include saving web pages in *.html format, printing their contents, and screen recording during the inspection of online resources. Proper documentation is crucial for subsequent forensic analysis and legal assessment of the suspect's actions[32].

Another key direction of ICFE is the recovery of previously deleted information that may hold evidentiary value in criminal proceedings. Through the use of specialized forensic software, such as EnCase, experts are able to restore deleted messages, files, and browser history data[33].

---

[31] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 48. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

[32] Казарян Е. Електронні (віртуальні) сліди в розслідуванні умисних убивств із мотивів расової, національної чи релігійної нетерпимості. *Актуальні питання судової експертизи і криміналістики* : зб. мат-лів міжнар. наук.-практ. конф. з нагоди 100-річчя Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» (м. Харків, 10 лист. 2023 р.). Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2023. С. 169.

[33] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 49. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

In addition, forensic specialists conduct comprehensive analyses of social media activity in order to identify a suspect's participation in groups promoting violence or intolerance, examine electronic communications, and establish individuals responsible for creating or disseminating hostile materials.

Given that content on social media platforms is frequently deleted, the timely appointment of a forensic examination is of critical importance. Investigators must ensure the immediate preservation of digital evidence and avoid any delay in transferring relevant materials to forensic experts.

In Ukraine, the aforementioned examinations are successfully conducted by a range of expert institutions, including forensic units of the Ministry of Internal Affairs, Research Institutes of Forensic Examinations under the Ministry of Justice, as well as duly certified private experts possessing the required qualifications and licenses. Effective cooperation between investigators and experts must be well-coordinated and carried out in strict compliance with procedural safeguards and confidentiality requirements.

It should also be noted that, in the context of martial law in Ukraine, there has been an observable increase in convictions for offences related to incitement to hatred and discrimination. In particular, between 2019 and 2024, a total of 45 convictions were delivered under Article 161 of the Criminal Code of Ukraine[34].

An analysis of judicial decisions in this category of cases demonstrates that investigative practice remains selective and uneven. A number of challenges arise in proving the constituent elements of such offences, including difficulties in establishing a motive of hatred or discrimination, which complicates the proper legal qualification of acts under Article 161 of the Criminal Code; inadequate documentation and preservation of digital evidence, potentially resulting in acquittals or case dismissals; and judicial difficulties in delineating the boundary between protected expression and statements that incur criminal liability. These issues underscore the relevance and practical significance of the present research and highlight the need for further scholarly development of the identified problems.

CONCLUSIONS

The conducted research made it possible to identify and specify the principal features of evidentiary processes in criminal proceedings concerning the use of hate speech in the digital environment. The proliferation of hate speech on the Internet, particularly on social media platforms, requires a comprehensive response from law enforcement authorities that combines digital forensic tools, forensic examinations, and effective legal mechanisms. Digital evidence serves as a key instrument for establishing the objective truth in such cases; at the same time, it is characterized by increased vulnerability to loss and alteration, as well as by the complexity of identifying its source. Particular importance attaches to the timely collection and preservation of electronic traces, ensuring their procedural admissibility, authenticity, and integrity, and compliance with standards for the preservation of digital information.

[34] Єдиний державний реєстр судових рішень. Офіційний сайт. URL: https://reyestr.court.gov.ua/.

The effective use of digital evidence in criminal proceedings related to hate speech necessitates further improvement of the regulatory framework, the development of unified methodological approaches to the collection and assessment of digital content, and the enhancement of interdisciplinary cooperation among investigators, prosecutors, judges, and experts. Establishing the motive of hatred as a mandatory element of the corpus delicti requires a comprehensive analysis of the content, the context of its dissemination, the behavioral characteristics of the individual, and their digital activity. It is also essential to take into account the case-law of the European Court of Human Rights concerning the assessment of contextual factors and the balance between freedom of expression and the prohibition of discrimination, thereby contributing to the consistency of judicial practice and the safeguarding of the principle of legal certainty.

Based on the findings of the study, it can be concluded that there is a need, first, to update (develop and refine) guidelines for investigators and experts working with digital evidence; second, to elaborate uniform approaches to the legal interpretation of hate speech; and third, to strengthen the specialization and professional training of participants in criminal proceedings in light of contemporary technological challenges. The implementation of these measures will enhance the effectiveness of investigations, ensure the proper substantiation of the motive of intolerance, and secure effective protection of human rights in the digital environment.

SUMMARY

The study examines the criminal procedural and forensic aspects of proving hate speech in the digital environment. The relevance of the topic is обусловед by the growing prevalence of discriminatory and xenophobic expressions on the Internet, particularly on social media platforms, as well as by the complexity of their proper legal qualification and evidentiary substantiation. The specific features of the formation and documentation of digital evidence are analyzed, including its vulnerability to loss or alteration, as well as the challenges associated with establishing authorship and the motive of intolerance. Particular attention is devoted to the role of forensic examinations and the application of digital forensic tools in criminal proceedings of this category. The importance of contextual assessment of statements and the necessity of maintaining a balance between freedom of expression and the prohibition of discrimination are also highlighted.

Based on the findings, the study substantiates the need to improve the regulatory framework, to develop unified methodological approaches to the documentation and evaluation of digital content, and to enhance interdisciplinary cooperation among participants in criminal proceedings. Directions are proposed for updating guidelines for investigators and experts and for elaborating uniform approaches to the legal interpretation of hate speech in accordance with international standards

References

1. Case of Norwood v. the United Kingdom (Applications no. 23131/03): Judgment European Court of Human Rights, 16 November 2004. URL: https://hudoc.echr.coe.int/eng?i=001-67632.

2. Case of Perinçek v. Switzerland (Applications no. 27510/08): Judgment European Court of Human Rights, 15 October 2015. URL: https://hudoc.echr.coe.int/eng?i=001-158235.

3. Case of Soulas and others v. France (Applications no. 15948/03): Judgment European Court of Human Rights, 10 October 2008. URL: https://globalfreedomofexpression.columbia.edu/cases/soulas-and-others-v-france/.

4. Case of Vejdeland and others v. Sweden (Applications no. 1813/07): Judgment European Court of Human Rights, 9 February 2012. URL: https://hudoc.echr.coe.int/fre?i=001-109046.

5. Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 47. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

6. Kazarian E. The use of special knowledge in the investigation of mu rders motivated by racial, national or religious intolerance. *Věda a perspektivy*. 2023. № 12 (31). P. 268–269. DOI: https://doi.org/10.52058/2695-1592-2023-12(31)-260-271.

7. Kondal M., Singh, V. Comparative analysis of tineye and google reverse image search engines. *International Journal of Innovative Science and Research Technology.* 2022. Vol. 7 (1). Pp. 205–207. DOI: https://doi.org/10.5281/zenodo.6378256.

8. Lyndon R., Tse V., Moore L., May-Hobbs M. Disinformation in Brazil: The 2019 Amazon fires on social media. In: Mair M., Meckin R., Elliot M. (Eds) *Investigative Methods: An NCRM Innovation Collection.* Southampton: National Centre for Research Methods. 2022. Pp. 44–53. DOI: https://doi.org/10.5258/NCRM/NCRM.00004547.

9. Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech. *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: https://search.coe.int/cm?i=0900001680a67955.

10. Reedy P. Interpol review of digitalevidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520. DOI: https://doi.org/10.1016/j.fsisyn.2020.01.015.

11. Spencer J. 101 social networking sites you need to know about in 2022. 2021. URL: https://makeawebsitehub.com/social-media-sites/.

12. Thouvenin F., Hettich P., Burkert H., Gasser U. 4 web archives. In: Remembering and Forgetting in the Digital Age. *Law, Governance and Technology Series.* 2018. Vol. 38. Springer, Cham. Pp. 84–101. DOI: https://doi.org/10.1007/978-3-319-90230-2_6.

13. Toktarova A., Syrlybay D., Myrzakhmetova B., Anuarbekova G., Rakhimbayeva G., Zhylanbaeva B., Suieuova N., Kerimbekov M. Hate Speech Detection in Social Networks using Machine Learning and Deep Learning Methods. *International Journal of Advanced Computer Science and Applications.* 2023. Vol. 14 (5). P. 396. DOI: https://doi.org/10.14569/IJACSA.2023.0140542.

14. Ziwen T., Channing Z. China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy.* 2021. Vol. 5 (1). Pp. 7–25. DOI: https://doi.org/10.69554/NATU8989.

15. Ажнюк Л. В. Лінгвістична експертиза як юридичний інструмент. *Магістеріум. Мовознавчі студії*. 2017. Вип. 66. С. 14.

16. Ажнюк Л., Ажнюк Б. Семантико-текстуальна лінгвістична експертиза усного й писемного мовлення: науково-методичні рекомендації. Київ, 2022. 47 с.

17. Єдиний державний реєстр судових рішень. Офіційний сайт. URL: https://reyestr.court.gov.ua/.

18. Казарян Е. Г. Поняття та особливості мови ворожнечі. *Х Юридичні могилянські читання – 2024 :* матеріали Х всеукраїнської наук.-практ. конф. (м. Миколаїв, 28 квіт. 2024 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2024. С. 23. URL: https://chmnu.edu.ua/wp-content/uploads/Mogilyanski_chitannya_-_2024.pdf.

19. Казарян Е. Г. Роль засобів цифрової криміналістики у розпізнаванні мови ворожнечі у соціальних мережах. *XI Юридичні могилянські читання – 2025* : матеріали XI всеукраїнської наук.-практ. конф. (м. Миколаїв, 24 квіт. 2025 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2025. С. 60–61. URL: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2794/1/XI%20Юридичні%20Могилянські%20читання.pdf.

20. Казарян Е. Електронні (віртуальні) сліди в розслідуванні умисних убивств із мотивів расової, національної чи релігійної нетерпимості. *Актуальні питання судової експертизи і криміналістики* : зб. мат-лів міжнар. наук.-практ. конф. з нагоди 100-річчя Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» (м. Харків, 10 лист. 2023 р.). Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2023. С. 169.

21. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Istoryko-pravovyi chasopys.* 2017. № 1 (9). С. 141.

22. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2022. № 4 (100). С. 230. DOI: https://doi.org/10.33766/2524-0323.100.226-236.

23. Коваль А. А. Петренко К. Д. Мова ворожнечі у цифровому просторі: особливості розслідування. *Вісник ЛННІ ім. Дідоренко*. 2025. Вип 3 (111). С. 97. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/80. DOI: https://doi.org/10.32782/2786-9156.111.3.

24. Коваль А. А. Толерантність онлайн: проблеми дотримання прав людини в соціальних мережах та правові шляхи їх вирішення. *Національні інтереси України*. №5 (10). 2025. С. 616. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-609-619.

25. Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 4 https://zakon.rada.gov.ua/laws/show/995004#Text.

26. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

27. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika:* XVIII. 2022. Т. 18. С. 32.

28. Національна поліція України. Офіційний сайт. URL: https://npu.gov.ua/.

29. Офіс Генерального прокурора. Офіційний сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

30. Рекомендація № R (97) 20 Комітету Міністрів державам-членам щодо «мови ненависті». *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech" – Freedom of Expression.

31. Черняк А. М. Використання спеціальних знань при дослідженні текстів, із закликами до підриву конституційного ладу, порушення територіальної цілісності і недоторканості України. *Вісник кримінального судочинства*. 2023. № 3–4. С. 106. DOI: https://doi.org/10.17721/2413-5372.2022.3-4/101-111.

Information about the authors:

Koval Alla Anatoliivna,
Doctor of Law, Professor,
Head of the Department of Constitutional
and Administrative Law and Procedure
Petro Mohyla Black Sea National University
10, 68 Desantnykiv St., Mykolaiv, 54000, Ukraine

Kazarian Eluchka Hurhenivna,
Doctor of Philosophy in Law,
Senior Lecturer of the Department of Constitutional
and Administrative Law and Procedure
Petro Mohyla Black Sea National University
10, 68 Desantnykiv St., Mykolaiv, 54000, Ukraine