UDC 343.14 + 343.982
DOI: 10.63341/naia-herald/2.2026.09

ISSN 2410-3594
E-ISSN 2786-7382

Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad

Valerii Khakhanovskyi*
Doctor of Law, Professor
National Academy of Internal Affairs, lawyer
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0001-5676-5641

Vitalii Petryk
Postgraduate Student
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0003-4723-7921

■ **Abstract.** As of 2025, over 94% of internet users use messaging apps on a monthly basis, leading to the growing role of electronic correspondence as a source of evidential information in criminal proceedings, particularly under martial law in Ukraine. The purpose of the study was to identify legal gaps in the regulation of messaging app correspondence as electronic evidence through a comparative analysis of the legal approaches of Ukraine, the United States of America, and the European Union. The study employed comparative legal and formal legal methods, along with the method of analysing judicial practice. The classification of messaging app correspondence was examined and systematised according to eight criteria, including the number of participants, access to correspondence, the format of information transmission, and the stage of creation. It was established that the current criminal procedural legislation of Ukraine does not distinguish a category of electronic evidence, whereas in the US, there is a developed system for the authentication of electronic evidence in accordance with the Federal Rules of Evidence, and the European Union adopted a dedicated Regulation (EU) 2023/1543 on cross-border access to electronic evidence in 2023. It was determined that Ukrainian courts generally recognise messaging correspondence as admissible evidence provided that the procedural rules for its collection are followed and there are no substantiated objections from the defence, although practice remains inconsistent. The grounds for deeming such correspondence inadmissible evidence have been analysed, including breaches of collection procedures, lack of confirmation of authorship, and the obtaining of evidence by unauthorised parties. The results of the study may be used by researchers, judges, prosecutors, and lawyers to improve the practice of working with electronic evidence in criminal proceedings, in addition to legislators for the regulatory framework of this institution

■ **Keywords:** digital forensics; admissibility of evidence; authentication; chain of custody; comparative legal analysis; procedural legislation

■ Introduction

The rapid development of digital technologies and the widespread use of mobile messaging apps have significantly altered the nature of public communication, shifting a substantial part of it into the digital sphere. As of 2025, the proportion of internet users who use messaging apps on a monthly basis exceeds 94%, with WhatsApp, Telegram, WeChat, and Messenger remaining the most popular platforms.

■ **Suggested Citation:**
Petryk, V., & Khakhanovsky, V. (2026). Messenger correspondence as electronic evidence in criminal proceedings in Ukraine and abroad. *Scientific Journal of the National Academy of Internal Affairs,* 31(2), 9-19. doi: 10.63341/naia-herald/2.2026.09.

■ *Corresponding author (*super-hvg@ukr.net*)

■ Received: 20.01.2026; Revised: 17.04.2026; Accepted: 26.05.2026; Published: 01.06.2026

Under martial law in Ukraine, the role of messaging apps has taken on particular importance: they have effectively become the primary, and in some cases the sole, means of communication between citizens, law enforcement agencies, and military units. Consequently, messaging app correspondence is increasingly emerging as a source of information regarding criminal offences, the circumstances of their planning and commission, and the circle of persons involved. However, the criminal procedure legislation of most states, including Ukraine, does not contain specific provisions regarding the procedure for collecting, recording, examining, and evaluating messaging app correspondence as electronic evidence. The absence of a unified regulatory approach leads to inconsistencies in judicial practice, which negatively affects the quality of evidence and the observance of the right to a fair trial. This necessitates a comprehensive comparative legal review aimed at identifying optimal approaches to the regulatory framework for this institution.

The issue of electronic evidence in criminal proceedings is the subject of active academic research both in Ukraine and abroad. For example, R. Stoykova (2021) identified three categories of unresolved threats to justice and the presumption of innocence when using digital evidence: inappropriate and inconsistent use of technology, outdated procedural safeguards that are not adapted to modern digital processes, and a lack of reliability checks in the practice of digital forensics. In a subsequent study, R. Stoykova (2023) argued that the right to a fair trial, enshrined in Article 6 of the European Convention on Human Rights[1], implicitly provides a conceptual framework for the development of universal rules regarding digital evidence at the investigation stage of criminal proceedings.

D. Wilson-Kovacs *et al.* (2023) examined the practice of defence lawyers in England and Wales regarding digital evidence and identified substantial difficulties in accessing, analysing, and presenting such evidence in court, specifically messages from WhatsApp and EncroChat. The authors concluded that improving lawyers' digital literacy is a key factor in ensuring the effective protection of clients' rights. S. Goodison *et al.* (2023), based on a survey of 50 prosecutors and 51 investigators in the United States, concluded that specialisation and continuous training play a critical role in working with digital evidence, emphasising that rapid technological changes require practitioners to constantly update their knowledge. A. Sachoulidou (2024) conducted a comprehensive analysis of the European Union's new legislation on cross-border access to electronic evidence – Regulation No. 2023/1543[2] and Directive No. 2023/1544[3] – and concluded that there has been a paradigm shift towards direct cooperation between competent national authorities and foreign service providers. V. Bajović & V. Ćorić (2025) analysed the judgment of the Court of Justice of the European Union of 30 April 2024 in Case No. C-670/22[4] (EncroChat) and its implications for the admissibility of intercepted messages from encrypted messaging services, in particular, regarding the requirements for a European Investigation Order. G. Horsman (2023), in a comprehensive Interpol review drawing on over 260 sources covering 2019-2022, noted major progress in the field of digital forensics, whilst highlighting unresolved issues regarding the standardisation and validation of methods for handling electronic evidence.

Among Ukrainian researchers, H. Avdieieva (2024) drew attention to issues related to the reliability and admissibility of electronic evidence in criminal proceedings, stressing the need to develop clear criteria for its assessment. T. Fomina & O. Rachynskyi (2023), having analysed investigative and judicial practice, concluded that there is an ambiguous understanding of the issue of collecting electronic evidence and proposed the use of the Berkeley Protocol[5] as a relevant tool in the context of armed aggression against Ukraine. I. Kalancha & D. Stemkovskyi (2025) conducted an examination of judicial practice regarding the use of electronic evidence in criminal proceedings in Ukraine and noted its inconsistency, providing recommendations for the development of a unified approach. A.M. Anheliuk (2023) reviewed problematic aspects of the use of electronic evidence in Ukrainian criminal procedural law, focusing on the practical difficulties of its application. P.Ye. Antoniuk & M.V. Hutsaliuk (2020) analysed the nature of electronic (digital) information as a source of evidence in criminal proceedings, justifying the need for its clear legal definition. I.V. Hora *et*

[1] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_004.

[2] Regulation of the European Parliament and of the Council No. 2023/1543 "On European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings". (2023, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543.

[3] Directive of the European Parliament and of the Council No. 2023/1544. (2023, July). Retrieved from https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng.

[4] Judgment of the Court of Justice of the European Union in Case C-670/22. (2024, April). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-670/22.

[5] Berkeley Protocol on Digital Open Source Investigations. (2022). Retrieved from https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.

al. (2024) investigated the place of digital forensics within the system of forensic knowledge, highlighting the emergence of a new scientific field directly related to the issue of electronic evidence.

Despite the significant contribution of the aforementioned researchers, a comprehensive comparative legal study of messaging app correspondence as a specific type of electronic evidence, considering the experience of various jurisdictions, has been overlooked, which defines the scientific novelty of the present work. The study aimed to identify legal gaps in the regulation of messaging app correspondence as electronic evidence in criminal proceedings through a comparative analysis of the legal approaches of Ukraine, the United States of America, and the European Union. The following tasks were formulated to achieve this goal: classify messaging app correspondence as electronic evidence; analyse judicial practice regarding the assessment of messaging app correspondence as evidence in criminal proceedings in Ukraine and abroad; formulate scientifically grounded proposals for improving criminal procedural legislation.

Materials and Methods

The study was conducted within the framework of the doctrine of admissibility of evidence in criminal proceedings, which is based on the principles of relevance, admissibility, reliability, and sufficiency of evidence, enshrined both in national legislation and in international standards of fair trial, in particular, in Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms[1]. A range of scientific research methods was employed in the study. The classification method was used to systematise types of messaging app correspondence according to various criteria. The comparative legal method was used to compare legal approaches to the regulation of electronic evidence, particularly messaging app correspondence, in Ukraine, the United States of America, and the European Union. This method allowed identifying common trends and significant differences in regulatory frameworks and judicial practice across different jurisdictions. The formal-legal (dogmatic) method was applied to analyse legislative acts: the Criminal Procedure Code of Ukraine[2], the Federal Rules of Evidence[3] (USA), Regulation No. 2023/1543[4], Directive EU No. 2023/1544[5], and Directive No. 2014/41/EU[6]. This method was used to identify gaps and conflicts in current legislation. The method of analysing case law was used to examine the decisions of Ukrainian and foreign courts. The source base of case law was compiled on the basis of decisions available in the Unified State Register of Court Decisions of Ukraine, decisions of the Court of Justice of the European Union, and decisions of Canadian courts.

The selection of court decisions was compiled according to the following principle: 12 court decisions from Ukrainian courts of various instances (district courts, courts of appeal, the Supreme Court, and the Grand Chamber of the Supreme Court) were selected, handed down between 2022 and 2025, in which the subject of assessment was messaging app correspondence as evidence in criminal proceedings. The chosen time frame is due to the fact that it was during this period, under martial law, that there was a substantial increase in the number of criminal proceedings in which electronic correspondence was used as key evidence. Decisions were selected from various regions of Ukraine (Zaporizhzhia, Odesa, Lviv, and Volyn regions, and the city of Kyiv) to ensure the representativeness of the sample, allowing for potential regional differences in legal practice to be taken into account. The decisions were selected using the keywords “messenger”, “electronic correspondence”, and “messenger correspondence” via the search engine of the Unified State Register of Court Decisions. For comparative analysis, the decision of the Court of Justice of the European Union in Case No. C-670/22[7] (EncroChat), and the decision of the Supreme Court of Canada in R. v. Mills[8], were additionally included. The scope of the sample allows for the identification of key trends and issues, but does not claim to be an exhaustive representation of all judicial practice.

[1] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_004.

[2] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[3] Federal Rules of Evidence of the United States. (2025, December). Retrieved from https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.

[4] Regulation (EU) 2023/1543 of the European Parliament and of the Council “On European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings”. (July 2023). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543.

[5] Directive of the European Parliament and of the Council No. 2023/1544. (2023, July). Retrieved from https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng.

[6] Directive of the European Parliament and of the Council No. 2014/41/EU. (2014, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041.

[7] Judgment of the Court of Justice of the European Union in Case No. C-670/22 (M.N. (EncroChat)). (2024, April). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-670/22.

[8] Judgment of the Supreme Court of Canada in Case “R. v. Mills”. (1999, November). Retrieved from https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1751/index.do.

Results

The variety of messaging applications and services, which differ in their properties and functionality, necessitates the systematisation of types of messaging in instant messengers. Such systematisation has not only theoretical but also direct practical significance, as the procedural order of its collection, methods of recording and criteria for assessing admissibility depend on the type of messaging. Based on the analysis conducted, a classification according to eight criteria is proposed, as presented in Table 1.

Table 1. Classification of messaging in instant messaging apps as electronic evidence

Classification criterion	Type	Characteristic
By number of participants	One-to-one chat (channel)	Involving one person
	Dialogue	Involving two participants
	Group chat	3 or more participants
By user access	Private	Invite-only or closed
	Public	Open to an unlimited number of people
By posting capability	Channels	Only authorised users can post
	Chats	Posting is available to all participants
By creation stage	Original	Stored on the original device
	Electronic copy	Photo, video, PDF, TXT, HTML formats
	Paper copy	Printouts of screenshots
By source	From the participant's device	Smartphone, computer, tablet
	From the service provider	Via the request mechanism
	From third parties	Persons aware of the correspondence
By format	Text	SMS, instant messaging apps, chats
	Multimedia	Photos, videos, audio, documents
By type of information	Content of correspondence	Text, files
	System information	Metadata: geolocation, date, time, IP
By response type	Chatbots	Automatic replies
	Artificial intelligence	AI for communication
	Live communication	Involving individuals

Source: developed by the authors

A systematic analysis of court decisions in criminal proceedings available in the Unified State Register of Court Decisions shows that courts generally recognise messaging app correspondence as admissible electronic evidence. The approaches of different courts to the assessment of this type of evidence vary significantly, indicating a lack of established practice and the need for its standardisation. Below are the most illustrative court decisions, which demonstrate both positive and negative practices regarding the recognition of messaging app correspondence as evidence.

In its Resolution of 12 June 2024 in Case No. 569/1908/23[1], the Supreme Court concluded that electronic (digital) evidence, in particular, materials from private messaging apps and Telegram channels, collected by operational units in compliance with the requirements of procedural law, constitute primary evidence in criminal proceedings concerning offences against the foundations of national security. This legal position of the Supreme Court is of fundamental importance, as it has, for the first time, clearly defined the status of electronic messages from messaging apps as primary, rather than merely supplementary, evidence in this category of criminal proceedings.

This conclusion has been applied in criminal cases No. 334/2045/24[2], No. 334/4126/24[3], No. 334/5278/24[4], No. 334/9999/23[5], in which the courts recognise the messaging correspondence submitted by the prosecution as admissible evidence

[1] Judgment of the Supreme Court of Ukraine in Case No. 569/1908/23. (2024, June). Retrieved from https://reyestr.court.gov.ua/Review/119741340.
[2] Judgments of Zaporizhzhia District Court in Cases No. 334/2045/24. (2024, December). Retrieved from https://reyestr.court.gov.ua/Review/123773129/.
[3] Judgments of Zaporizhzhia District Court in Cases No. 334/4126/24. (2024, December). Retrieved from https://reyestr.court.gov.ua/Review/123645637.
[4] Judgments of Zaporizhzhia District Court in Cases No. 334/5278/24. (2024, November). Retrieved from https://reyestr.court.gov.ua/Review/123523319.
[5] Judgments of Zaporizhzhia District Court in Cases No. 334/9999/23. (2024, August). Retrieved from https://reyestr.court.gov.ua/Review/121038824.

subject to two conditions: compliance with the legal requirements regarding the procedure for gathering evidence and the form of recording (inspection reports, attachments in the form of screenshots or files), in addition to the defence's inability to refute this evidence. In the judgment of the Khortytskyi District Court of Zaporizhzhia dated 6 January 2025 in case No. 337/862/23[1], the court assessed the messaging correspondence as proper, admissible, and reliable evidence, which, taken together with other evidence, proves the circumstances of the criminal offence beyond a reasonable doubt.

Nonetheless, there are frequent instances of courts rejecting messenger correspondence on the grounds specified in Articles 86 and 87 of the Code of Criminal Procedure of Ukraine[2]. Specifically, in its judgment of 29 February 2024, the Rozdilnyanskyi District Court of Odesa Region in Case No. 511/563/19[3] concluded that all evidence obtained during the pre-trial investigation was inadmissible, as the investigation had been conducted without a proper authorisation order. In the judgment of the Zhovkivsky District Court of Lviv Region dated 8 March 2024 in case No. 461/3477/22[4], the court noted that the reference to the report on the examination of mobile phones was procedurally incorrect, as no expert opinions had been provided to confirm that the correspondence via messaging app was indeed sent by the defendant.

It is also worth noting the ruling of the Appeals Chamber of the High Anti-Corruption Court dated 1 February 2022, No. 991/492/19[5], in which the court ruled that evidence gathered by investigators from the Territorial Department of the State Bureau of Investigation was inadmissible, on the grounds that it had been obtained by unauthorised persons in breach of the procedure established by law. Furthermore, the Grand Chamber of the Supreme Court, in its ruling of 21 June 2023 in case No. 916/3027/21[6], concluded that messages sent via messaging apps constitute electronic evidence, which is assessed by the court according to its internal conviction in conjunction with other evidence. However, the court may consider electronic correspondence as evidence only if it allows establishing the authors and the content of the correspondence.

In its judgment of 18 July 2024, the Turka District Court of Lviv Region in Case No. 458/465/22[7] rejected the prosecution's evidence, noting that the information in the screenshots did not allow for the unequivocal identification of the application, the authors, the time of the correspondence, or the connection between the content and the incident. The court concluded that electronic correspondence constitutes neither written nor electronic evidence to substantiate the commission of a crime. This decision illustrates a situation where the absence of clear regulatory criteria for assessing electronic evidence leads to its complete rejection by the court.

A summary of the analysed court decisions allows identifying the following main grounds for deeming messaging app correspondence inadmissible evidence: firstly, a breach of the procedural rules for gathering evidence, in particular, the absence of a proper order or the conduct of investigative actions by unauthorised entities; secondly, the lack of confirmation of the authorship of the messages, i.e. the inability to unequivocally establish that the defendant is the author of specific messages; thirdly, the failure to provide expert opinions on the authenticity and integrity of the electronic data; fourthly, the submission of evidence in a form that does not allow its origin and connection to the criminal offence to be established. Conversely, the admissibility of correspondence correlates with compliance with the procedural rules for recording, the existence of inspection reports with annexes, and the absence of substantiated objections from the defence.

In the legal system of the United States of America, the admissibility of electronic evidence, including instant messages and text messages, is governed by the Federal Rules of Evidence (FRE)[8]. Unlike Ukrainian legislation, the FRE contain clear rules of authentication applicable to all types of electronic evidence. Under Rule 901(a), the party presenting the evidence must provide sufficient grounds for concluding that

[1] Judgment of Khortytskyi District Court of Zaporizhzhia in Case No. 337/862/23. (2025, January). Retrieved from https://reyestr.court.gov.ua/Review/121038828.
[2] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[3] Judgment of Rozdilnianskyi District Court of Odesa Oblast in Case No. 511/563/19. (2024, February). Retrieved from https://reyestr.court.gov.ua/Review/117324337.
[4] Judgment of Zhovkivskyi District Court of Lviv Oblast in Case No. 461/3477/22. (2024, March). Retrieved from https://reyestr.court.gov.ua/Review/117517325.
[5] Ruling of the Appellate Chamber of the High Anti-Corruption Court in Case No. 991/492/19. (2022, February). Retrieved from https://reyestr.court.gov.ua/Review/103002653.
[6] Resolution of the Grand Chamber of the Supreme Court of Ukraine in Case No. 916/3027/21. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/112088045.
[7] Judgment of Turkivskyi District Court of Lviv Oblast in Case No. 458/465/22. (2024, July). Retrieved from https://reyestr.court.gov.ua/Review/120455406.
[8] Federal Rules of Evidence of the United States. (2025, December). Retrieved from https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.

the evidence is what the presenter claims it to be. Rule 901(b) provides ten non-exhaustive examples of methods of authentication, including: the testimony of a knowledgeable person (Rule 901(b)(1)), distinctive features of the content and other distinguishing characteristics (Rule 901(b)(4)), including metadata.

The decision in Lorraine v. Markel American Insurance Co.[1] is of fundamental importance to the practice of electronic evidence admissibility in the United States, in which Judge P. Grimm conducted an exhaustive analysis of five consecutive standards of admissibility: relevance (Rule 401), authenticity (Rule 901), absence of hearsay or application of exceptions (Rules 801-807), compliance with rules regarding the original (Rules 1001-1008), and the balance between probative value and bias (Rule 403). The court emphasised that the metadata of electronic documents (date, time, author identification) are distinctive characteristics that may be used for authentication under Rule 901(b)(4). This decision is recognised as a fundamental benchmark for the practice of admissibility of electronic evidence in US federal courts.

Notably, state courts have developed an approach to authenticating text messages through so-called "confirming circumstances", which include: registration of the mobile device in the defendant's name, password protection, the use of characteristic nicknames, and content consistent with the circumstances of the case. The courts consistently confirm that the mere fact of the sender's name being indicated in the message is insufficient for authentication; additional confirming circumstances are required, which is consistent with the approach of Ukrainian courts. A key difference between the US system and the Ukrainian one is that the Federal Rules of Evidence (FRE) also provide for the possibility of self-authentication of electronic records under Rule 902(13)-14, added in 2017, which allows electronic records to be recognised as authentic without additional evidence, provided there is certification by a qualified expert. Such a possibility is absent in Ukrainian procedural law, which complicates the burden of proof and increases the burden on the prosecution. These trends in the practice of federal courts are confirmed by a study by M. Novak (2020), who, having analysed the practice of US courts of appeal, noted an increase in the number of cases in which digital evidence plays a key role, and highlighted current issues regarding its admissibility and authentication.

In 2023, the European Union adopted Regulation No. 2023/1543[2], which enters into force on 18 August 2026. The Regulation establishes rules under which a judicial authority of one Member State may directly request electronic evidence from a service provider in another Member State, regardless of where the data is stored. The service provider is obliged to comply with the Production Order within 10 days, and in urgent cases within 8 hours. Of fundamental importance for the practice regarding the admissibility of intercepted messages from encrypted messaging services is the judgment of the Court of Justice of the European Union of 30 April 2024 in Case C-670/22 (EncroChat)[3]. In that case, the Court of Justice of the European Union held that a European Investigation Order (EIO) for the purpose of obtaining evidence already in the possession of the executing Member State may be issued only by a competent authority in accordance with the national law of the issuing state. The EncroChat case concerned the mass interception of messages from an encrypted messaging service used by organised criminal groups. In 2020, French and Dutch law enforcement agencies installed malware on EncroChat's servers, gaining access to millions of messages which were subsequently transferred to law enforcement agencies in other EU Member States via the EIO mechanism.

In parallel with the EU Regulation, the United States of America adopted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018[4], which allows US law enforcement agencies to request data from American technology companies regardless of where the data is stored. Both instruments, the EU Regulation and the CLOUD Act, depart from the principle whereby jurisdiction is determined by the physical location of data storage, reflecting a global trend towards simplifying cross-border access to electronic evidence. For Ukraine, this trend is of particular significance, as the servers of most popular messaging apps (Telegram, WhatsApp, Signal) are located abroad, which greatly complicates the procedure for obtaining electronic evidence through the mechanism of international legal assistance. Currently, Ukrainian legislation does not provide for a mechanism for direct access to foreign service providers, which necessitates the integration of relevant provisions.

[1] Judgment of the United States District Court, D. Maryland in Case "Lorraine v. Markel American Insurance Co.". (2007, May). Retrieved from https://app.minerva26.com/case_law/17344-lorraine-v-markel-am-ins-co.
[2] Regulation of the European Parliament and of the Council No. 2023/1543 "On European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings". (2023, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543.
[3] Judgment of the Court of Justice of the European Union in Case No. C-670/22 (M.N. (EncroChat)). (2024, April). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-670/22.
[4] Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of U.S. (2018, March). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/4943.

The Supreme Court of Canada, in the case of R. v. Mills[1], concluded that electronic correspondence is admissible evidence, and a copy of such correspondence captured in a screenshot is also deemed admissible, provided its authenticity is confirmed. The Canadian approach is characterised by pragmatism, as the court assesses, first and foremost, the reliability and credibility of the evidence rather than formal compliance with procedural requirements, which differs from the more formalised approach in both Ukraine and the US.

In the UK, the admissibility of digital evidence is governed primarily by the exclusion rules set out in the Police and Criminal Evidence Act 1984 (PACE)[2]. British courts take a flexible approach, assessing three aspects of potential evidence: relevance, reliability, and fairness of its use. The practice of using EncroChat data in UK criminal cases has demonstrated that intercepted messages from encrypted messaging apps are recognised as admissible evidence provided the procedure for obtaining them is followed. However, British defence lawyers face significant difficulties in challenging the reliability of such evidence due to limited access to technical information regarding the methods used to intercept it.

Thus, a comparative analysis of the legislation and practice across four jurisdictions allows for the identification of three main approaches to the regulation of electronic evidence from messaging apps. The first is the formalised approach (US), under which authentication is performed in accordance with codified rules with clear admissibility criteria. The second is the pragmatic approach (UK, Canada), under which the court assesses evidence on the basis of its substance and reliability, rather than formal criteria. The third is the EU's combined approach, which provides for regulatory control at the supranational level (Regulation 2023/1543) with the discretion of national courts regarding the assessment of admissibility. Ukraine currently leans towards the pragmatic approach, but without an adequate regulatory framework, which creates uncertainty and inequality in the application of the law.

Based on the comparative analysis conducted, the need to improve Ukraine's criminal procedural legislation is substantiated. In particular, it is proposed to amend Article 99 of the CPC of Ukraine[3] by introducing a definition of electronic evidence that would cover information in electronic (digital) form contained on electronic media, including correspondence in messaging apps. Furthermore, it is advisable to include a separate Article in Chapter 15 of the CPC of Ukraine regarding the procedure for temporary access to electronic communications, as well as to amend Articles 86-87 of the CPC of Ukraine, establishing specific requirements for the procedure for collecting and recording electronic evidence, specifically the mandatory recording of metadata (date, time, IP address, device and account identifiers). The experience of the US, where the FRE Rule 902(13)-14[4] provides for the self-authentication of electronic records, and the EU, where Regulation No. 2023/1543[5] establishes clear timeframes and procedures for the production of electronic evidence, can be cited as confirmation of the advisability of such changes.

Discussion

The results of this study allow for a comparative analysis with the findings of other researchers and reveal both similarities and differences in the understanding of the issue of using messaging app correspondence as electronic evidence. One of the key issues identified during the analysis of Ukrainian judicial practice is the lack of a uniform approach to the authentication of electronic messages. Ukrainian courts assess messaging app correspondence primarily "in conjunction with other evidence", which does not always ensure proper verification of authenticity. The conclusions drawn by R. Stoykova (2023) regarding the need to develop fair trial-based rules for digital evidence are relevant, as the results of this study confirm that the absence of clear regulatory requirements for the authentication of messaging leads to inconsistencies in judicial practice. Unlike in Ukraine, the United States of America has a systematic approach to authentication, enshrined in Federal Rule of Evidence 901, which includes specific methods for verifying the authenticity of electronic communications. The reason for these discrepancies lies in the fact that the American legal system has a long-standing tradition of regulatory control over electronic evidence, whereas in Ukraine, the development of the relevant legal framework has only just begun.

[1] Judgment of the Supreme Court of Canada in Case "R. v. Mills". (1999, November). Retrieved from https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1751/index.do.
[2] Police and Criminal Evidence Act 1984 (PACE) of United Kingdom. (1984, October). Retrieved from https://www.legislation.gov.uk/ukpga/1984/60.
[3] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[4] Federal Rules of Evidence of the United States. (2025, December). Retrieved from https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.
[5] Regulation of the European Parliament and of the Council No. 2023/1543 "On European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings". (2023, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543.

The findings of D. Wilson-Kovacs *et al.* (2023) regarding the difficulties faced by defence lawyers when dealing with digital evidence are consistent with the results of this analysis. In particular, the cases examined revealed that the defence often fails to file motions requesting an expert examination of electronic evidence or seeking to have it declared inadmissible, which effectively facilitates the court's acceptance of such evidence. However, the analysis also reveals a different picture: in cases where the defence actively contested the authenticity and authorship of correspondence (in the case of the Zhovkivsky District Court of Lviv Region), the courts concluded that such evidence was inadmissible. This confirms the thesis of the aforementioned researchers regarding the critical role of digital literacy among lawyers in ensuring fair trial proceedings.

The results of a comparative analysis with EU legislation confirm the conclusions of A. Sachoulidou (2024) regarding a paradigm shift towards direct cooperation with service providers. Regulation No. 2023/1543[1] sets specific deadlines for the execution of Production Orders, which differs significantly from Ukrainian practice, where obtaining electronic evidence from messaging service providers remains a lengthy and informalised process. The statements of H. Avdieieva (2024) regarding the reliability of digital evidence in criminal proceedings are well-founded, as the findings of this study further confirm that Ukrainian courts face difficulties in assessing the reliability of messaging correspondence, particularly when it is submitted in the form of screenshots without metadata.

An analysis of the EncroChat[2] case and the conclusions of V. Bajović & V. Ćorić (2025) demonstrate that the issue of the admissibility of intercepted messages from encrypted messaging apps is relevant not only for Ukraine but also for the entire European Union. The EU Court's ruling established important procedural safeguards regarding the issuance of EIOs, which may serve as a benchmark for the development of Ukrainian legislation in the field of international cooperation in the collection of electronic evidence, the importance of which was underlined by N. Akhtyrska (2022). In this context, a study by N. Akhtyrska & O. Kostiuchenko (2022) is also notable, devoted to the procedural and organisational aspects of gathering electronic evidence within the framework of international cooperation, which further confirms the complexity and multifaceted nature of the problem of cross-border acquisition of digital evidence.

The observation by O. Harasymiv *et al.* (2023) regarding the lack of clarity in understanding the difference between written and electronic evidence is corroborated by the court decisions analysed. In the case of the Turka District Court of Lviv Region, the court concluded that electronic correspondence is "neither written nor electronic evidence", which clearly illustrates the problem highlighted by the aforementioned researchers. The conclusions of these authors, considering the results of this study, can be viewed from a different perspective: the problem lies not so much in a vague understanding of the difference, but in the absence of a statutory definition of electronic evidence in the Code of Criminal Procedure of Ukraine, which deprives the courts of a clear guideline.

The recommendations of T. Fomina & O. Rachynskyi (2023) on the use of the Berkeley Protocol[3] appear reasonable, but require adaptation to the specific nature of messaging app correspondence, as the protocol was developed primarily for the verification of open-source intelligence (OSINT), whereas messaging app correspondence is, by its very nature, closed and requires specific access procedures. I.V. Basysta & L.V. Havryliuk (2024) investigated the practice of using digital data from open sources in the investigation of criminal offences, outlining both the potential and the procedural difficulties of such an approach.

Nonetheless, the results of a comparative analysis indicate that the most effective path to improvement is a comprehensive approach that combines the statutory codification of requirements for electronic evidence (following the example of the FRE in the US), mechanisms for cross-border access (following the example of the EU Regulation), and the development of specialisation among law enforcement officers and judges in the field of digital evidence (in accordance with the recommendations of S.E. Goodison *et al.* (2023).

Particular attention is drawn to the issue of classifying messaging app correspondence, as proposed within this study. The identification of eight classification criteria (based on the number of participants, access, storage capability, creation stage, source of origin, format, type of information, and method of response) constitutes an original contribution that builds upon the approaches of A. Kovalenko (2023) regarding the classification of digital traces of criminal offences. However, whilst A. Kovalenko (2023)

[1] Regulation of the European Parliament and of the Council No. 2023/1543 "On European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings". (2023, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543.

[2] Judgment of the Court of Justice of the European Union in Case No. C-670/22 (M.N. (EncroChat)). (2024, April). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-670/22.

[3] Berkeley Protocol on Digital Open Source Investigations. (2022). Retrieved from https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.

concentrated on the technical characteristics of digital traces in general, the classification in this study is specifically oriented towards the procedural significance of different types of correspondence, which has direct practical value for judges and lawyers when assessing the admissibility of a specific type of digital evidence.

The three approaches to the regulation of electronic evidence identified in the study, formalised (USA), pragmatic (UK, Canada), and combined (EU), are consistent with the findings of K. Ligeti *et al.* (2021) regarding the diversity of admissibility standards across EU member states. Thereby, K. Aksamitowska (2021), having examined the practice of using digital evidence in the investigation of international crimes in Germany, Sweden, Finland and the Netherlands, demonstrated that even in states with developed legal systems, significant procedural challenges remain when dealing with electronic evidence, which reinforces the conclusion regarding the universal nature of the identified issues. For Ukraine, which is in the process of harmonising its legislation with the EU acquis, a combined approach appears to be the most promising, as it allows for the combination of clear regulatory frameworks with the flexibility of judicial discretion. The practical implementation of this approach requires both legislative changes (amendments to the Code of Criminal Procedure of Ukraine) and the development of specialised training for judges, prosecutors, and lawyers in the field of working with digital evidence.

■ Conclusions

The subject of the study was messaging app correspondence as electronic evidence in criminal proceedings. The objective set – to identify legal gaps in the regulation of this type of evidence through a comparative analysis of the legal approaches of Ukraine, the US and the EU – was achieved through a comprehensive analysis of legislative acts, judicial practice, and academic publications. It was established that messaging constitutes a distinct category of electronic evidence, characterised by specific features: creation and modification using computer devices, storage on various media and providers' servers, the ability to be reproduced multiple times without loss of quality, and increased vulnerability to modification and destruction. The author proposes a classification of messaging based on eight criteria, which is of practical significance for determining the procedural status of a specific type of electronic evidence. An analysis of the legislation helped establish that the current Code of Criminal Procedure of Ukraine does not contain specific provisions regarding electronic evidence; in particular, it does not define the concept of electronic evidence nor does it establish special requirements for the procedure for collecting, recording and assessing correspondence in messaging apps, whereas in the US and the EU, the relevant legal frameworks are significantly more developed. The results of the study showed that Ukrainian courts generally recognise messaging correspondence as admissible evidence provided that procedural rules are followed and there are no well-founded objections from the defence; however, practice remains inconsistent, as evidenced by diametrically opposed decisions by different courts on similar issues. Such data indicate the need for clear rules governing the handling of electronic evidence to be enshrined in legislation. The analysis identified key grounds for deeming correspondence inadmissible: breaches of collection procedures, lack of confirmation of authorship, evidence obtained by unauthorised parties, and the submission of evidence in a form that does not allow its origin to be established. A comparative analysis established that the systematic approach to authentication developed in the US (FED Rule 901) and the mechanisms for cross-border access provided for in Regulation No. 2023/1543 can serve as a benchmark for the development of Ukrainian legislation. The results obtained suggest that the proposed amendments to Article 99, Chapter 15, and Articles 86-87 of the Code of Criminal Procedure of Ukraine will contribute to the formation of a uniform judicial practice and improve the quality of evidence.

In summary, the effective use of messaging app correspondence as electronic evidence requires a comprehensive approach combining regulatory frameworks, the development of specialisation among law enforcement officers and judges, and international cooperation. Conceptually, the above indicates the emergence of a new institution of electronic evidence in criminal proceedings, which requires both theoretical justification and practical testing.

A limitation of the study was the relatively small sample size of court decisions (12 cases) and the lack of full texts of some decisions in the public domain. Promising areas for further research include an empirical examination of the practice of collecting electronic evidence by Ukrainian law enforcement agencies and the development of methodological guidelines for judges on assessing the authenticity of messaging app correspondence using specialist knowledge.

■ Acknowledgements

None.

■ Funding

None.

■ Conflict of Interest

None.

References

[1] Akhtyrska, N.M. (2022). Obtaining evidence in electronic form in the light of the Second Additional Protocol to the Convention on Cybercrime. *Criminalistics and Forensic Expertise*, 67, 188-200. doi: 10.33994/kndise.2022.67.21.

[2] Akhtyrska, N.M., & Kostiuchenko, O.Yu. (2022). Procedural and organizational aspects of collecting electronic evidence during international cooperation. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 72(2), 192-198.

[3] Aksamitowska, K. (2021). Digital evidence in domestic core international crimes prosecutions: lessons learned from Germany, Sweden, Finland and the Netherlands. *Journal of International Criminal Justice*, 19(1), 189-211. doi: 10.1093/jicj/mqab035.

[4] Anheliuk, A.M. (2023). The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues). *Scientific Bulletin of Uzhhorod National University. Series: Law*, 79(2), 214-218. doi: 10.24144/2307-3322.2023.79.2.32.

[5] Antoniuk, P.Ye., & Hutsaliuk, M.V. (2020). On the essence of electronic (digital) information as a source of evidence in criminal proceedings. *Criminalistic Bulletin*, 33(1), 37-49. doi: 10.37025/1992-4437/2020-33-1-37.

[6] Avdieieva, H.K. (2024). Problems of determining the reliability of digital evidence in criminal proceedings. *Bulletin of LNDI named after E.O. Didorenko*, 1(105), 33-48. doi: 10.33766/2786-9156.105.

[7] Bajović, V., & Ćorić, V. (2025). EncroChat and Sky ECC data as evidence in criminal proceedings in light of the CJEU decision. *European Journal of Crime, Criminal Law and Criminal Justice*, 33, 235-262. doi: 10.1163/15718174-bja10062.

[8] Basysta, I.V., & Havryliuk, L.V. (2024). Use of digital data from open sources during the investigation of criminal offenses: Selected aspects. *Scientific and Informational Bulletin of Ivano-Frankivsk University of Law*, 17(29), 227-243. doi: 10.33098/2078-6670.2024.17.29.227-243.

[9] Fomina, T.H., & Rachynskyi, O.O. (2023). Electronic evidence in criminal proceedings: Problematic issues of theory and practice. *Bulletin of Kharkiv National University of Internal Affairs*, 102(3), 207-220. doi: 10.32631/v.2023.3.43.

[10] Goodison, S.E., Davis, R.C., & Jackson, B.A. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, 6, article number 100319. doi: 10.1016/j.fsisyn.2023.100319.

[11] Harasymiv, O.I., Marko, S.I., & Riashko, O.V. (2023). Digital evidence: some problematic issues regarding their concept and use in criminal justice. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 75(2), 158-162. doi: 10.24144/2307-3322.2022.75.2.25.

[12] Hora, I.V., Kolesnyk, V.A., & Popovych, I.I. (2024). On the issue of digital forensics in the system of forensic knowledge. *Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence*, 68, 86-91. doi: 10.32782/2307-1745.2024.68.18.

[13] Horsman, G. (2023). Interpol review of digital evidence for 2019-2022. *Forensic Science International: Synergy*, 6, article number 100313. doi: 10.1016/j.fsisyn.2022.100313.

[14] Kalancha, I.H., & Stemkovskyi, D.B. (2025). Use of evidence in electronic form in the criminal process of Ukraine: Judicial practice. *Analytical and Comparative Jurisprudence*, 2, 1001-1008. doi: 10.24144/2788-6018.2025.02.148.

[15] Kovalenko, A.V. (2023). Classification of electronic (digital) traces of criminal offenses. *Problems of Legality*, 161, 202-214. doi: 10.21564/2414-990X.161.278117.

[16] Ligeti, K., Garamvölgyi, B., Ondrejová, A., & Galen, M. (2021). Admissibility of evidence in criminal proceedings in the EU. *Eucrim: The European Criminal Law Associations' Forum*, 3, 201-208. doi: 10.30709/.

[17] Novak, M. (2020). Digital evidence in criminal cases before the U.S. Courts of Appeal: Trends and issues for consideration. *Journal of Digital Forensics, Security and Law*, 14(4).

[18] Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift. *New Journal of European Criminal Law, 2024, 256-274*. doi: 10.1177/20322844241258649.

[19] Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, article number 105575. doi: 10.1016/j.clsr.2021.105575.

[20] Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law and Security Review*, 49, article number 105801. doi: 10.1016/j.clsr.2023.105801.

[21] Wilson-Kovacs, D., Helm, R., Growns, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *The International Journal of Evidence & Proof*, 27(3). doi: 10.1177/13657127231171620.

Листування в месенджері як електронний доказ у кримінальному судочинстві України та закордоном

Валерій Хахановський
Доктор юридичних наук, професор
Національної академії внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0001-5676-5641
Віталій Петрик
Аспірант
Національної академії внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0003-4723-7921

■ **Анотація.** Станом на 2025 рік понад 94 % користувачів мережі Інтернет щомісяця використовують месенджери, що зумовлює підвищення ролі електронного листування як джерела доказової інформації в кримінальних провадженнях, зокрема в умовах воєнного стану в Україні. Метою дослідження було виявлення правових прогалин у регулюванні листування в месенджерах як електронного доказу шляхом порівняльного аналізу правових підходів України, Сполучених Штатів Америки та Європейського Союзу. У процесі дослідження було використано порівняльно-правовий, формально-юридичний методи, а також метод аналізу судової практики. Було досліджено та систематизовано класифікацію листування в месенджерах за вісьмома критеріями, зокрема за кількістю учасників, доступом до листування, форматом передання інформації та етапом створення. Встановлено, що чинне кримінальне процесуальне законодавство України не виокремлює категорію електронних доказів, тоді як у Сполучених Штатах Америки є розвинена система автентифікації електронних доказів відповідно до Federal Rules of Evidence, а Європейський Союз 2023 року ухвалив спеціалізований Регламент (EU) 2023/1543 про транскордонний доступ до електронних доказів. Виявлено, що українські суди здебільшого визнають листування в месенджерах допустимим доказом за умови дотримання процесуального порядку збирання й за відсутності обґрунтованих заперечень сторони захисту, однак практика є суперечливою. Проаналізовано підстави визнання такого листування недопустимим доказом, зокрема порушення процедури збирання, неможливість підтвердження авторства й отримання доказів неуповноваженими суб'єктами. Результати дослідження можуть бути використані науковцями, суддями, прокурорами та адвокатами для вдосконалення практики роботи з електронними доказами в кримінальних провадженнях, а також законодавцем для нормативного врегулювання цього інституту

■ **Ключові слова:** цифрова судова експертиза; допустимість доказів; автентифікація; ланцюг збереження доказів; порівняльний правовий аналіз; процесуальне законодавство