Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 107-113

Electronic Evidence in Criminal and Civil Proceedings: Technologies, Challenges and Perspectives

Sandra Kaija
Riga Stradiņš University
Riga, Latvia,
ORCID 0000-0002-2711-613X

Inga Kudeikina
Riga Stradiņš University
Riga, Latvia
ORCID 0000-0002-7895-4264

Abstract. **In the contemporary digital environment, electronic evidence has become a fundamental element in both criminal and civil proceedings. The accelerated evolution and pervasive integration of information technologies into routine activities, communication, and business processes has led to a substantial augmentation in the volume and significance of digital data as potential evidence. This evolution has created a pressing need for a coherent, consistent, and technologically informed legal framework to regulate the collection, preservation, evaluation, and admissibility of electronic evidence in judicial proceedings.**

Notwithstanding the ongoing evolution of the legal landscape, the utilisation of electronic evidence continues to be encumbered by a plethora of intricate challenges. These include the authentication, integrity, and reliability of digital data, as well as the mitigation of risks associated with data manipulation, cybersecurity threats, and cross-border data access. Furthermore, discrepancies in procedural regulations between criminal and civil proceedings have the potential to result in inconsistencies in the handling and assessment of electronic evidence.

The present article undertakes a comparative analysis of the legal framework governing electronic evidence in both criminal and civil contexts, with a view to identifying common principles and key distinctions. Furthermore, it delves into pertinent jurisprudence, emphasising existing regulatory lacunae and practical challenges that emerge in the implementation of legal standards within technologically sophisticated settings.

The objective of the present article is twofold. Firstly, the present study seeks to analyse the current legal regulation of electronic evidence and its alignment with technological realities. Secondly, it evaluates the challenges encountered during its application and proposes directions for improvement. It is imperative to emphasise the importance of enhancing legal certainty, procedural fairness, and the effective integration of technological solutions in evidence handling processes. The study emphasises the necessity of a balanced approach that ensures both the reliability of electronic evidence and the protection of fundamental rights in judicial proceedings.

The present study employs a combination of descriptive, analytical, deductive and inductive methods. The descriptive method is utilised to present the nature of electronic evidence, the legal and technical details of its acquisition and use. The analytical method is employed to examine in depth the existing laws and regulations and their interpretation in jurisprudence, and to identify problems. Deductive and inductive methods are used to express conclusions and suggestions. The deductive method is employed to analyse the application of general rules in specific situations involving electronic evidence, while the inductive method is used to formulate general conclusions and recommendations for improving the legal framework for electronic evidence by examining specific court rulings and legal experts' findings.

Keywords – electronic evidence, admissibility of evidence, technologies, digital forensics

I. Introduction

In the digital age, electronic evidence assumes an increasingly pivotal role in both criminal and civil proceedings. Technological advancements in the realm of information creation, storage, and transmission are profoundly reshaping the landscape of justice. Consequently, legal systems worldwide are confronted with substantial challenges in ensuring the reliability, admissibility, and effective utilisation of electronic evidence within judicial processes.

The term 'electronic evidence' encompasses a vast array of digital data, including emails, text messages, social media content, metadata, cloud-stored files, and information extracted from electronic devices. In contradistinction to conventional forms of evidence, digital data is highly volatile, readily alterable or deleteable, and necessitates specialised forensic techniques to ensure its integrity and authenticity. Consequently, courts and legal practitioners must adapt to the complexities of handling such evidence while maintaining fundamental legal

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.98

principles, such as fairness, due process, and the protection of individual rights. Despite the existence of legal frameworks regulating electronic evidence, various challenges persist. These include inconsistencies in legislation, difficulties in cross-border data access, privacy concerns, and the need for clear guidelines on admissibility criteria. Furthermore, the rapid evolution of technology raises ongoing questions about how legal norms should be adjusted to address new forms of digital evidence, such as blockchain records, artificial intelligence-generated data, and encrypted communications.

The objective of this article is to analyse the current legal regulation of electronic evidence and its alignment with technological realities, while also evaluating the challenges encountered in its application and propose possible directions for improvement. By assessing existing laws, court practices, and expert opinions, this research seeks to provide valuable insights into how electronic evidence can be more effectively integrated into the judicial process.

II. ELECTRONIC EVIDENCE – REGULATORY CHALLENGES

The right to a fair trial is considered a fundamental human right by both international law and the national law of every democratic country. Evidence plays an important role in ensuring this right, although there is no uniform legal definition of the concept of "proof". Its content must be disclosed in the context of an analysis of procedural law. For instance, Section 127, Paragraph one of the Criminal Procedure Law stipulates that "evidence in criminal proceedings is any information obtained in accordance with the procedures prescribed by law and corroborated in a specific procedural form regarding facts […]" [16], while Section 92, Paragraph one of the Civil Procedure Law states that "evidence is information on the basis of which the court determines the existence or absence of facts which are relevant for the adjudication of the case" [3]. A literal interpretation of the term leads to the conclusion that, more broadly, the term "evidence" is used in the legal protection system to designate anything used to prove that something else is true or exists, from witness statements to documents, objects, etc. [21].

The legislation does not provide for a predetermined set of items of information to be regarded as evidence. The court retains the prerogative to determine the admissibility of evidence, through the application of quantitative and qualitative analysis to news reports. This position has been endorsed by the Senate of the Republic of Latvia, which has asserted that the evaluation of evidence falls within the purview of the court [18].

Simultaneously, it is important to acknowledge that the legislature did not entrust the evaluation of the evidence to the court's discretion, but rather delineated the criteria to be fulfilled when assessing the submitted information. In other words, the information becomes evidence when it fulfils the specified criteria. It is imperative to acknowledge that the evaluation of evidence is not left to the court's discretion, but rather, it is subject to specific criteria that must be met for its admissibility in court proceedings. These criteria, outlined in sections 130 of the Criminal Procedure Law and 95 of the Civil Procedure Law, serve to ensure the integrity and reliability of the evidence presented. Consequently, it can be concluded that the assessment of evidence is a cognitive process, constituting a legal act undertaken by the court through the application of principles of logic and law. In terms of its internal content, this process may be described as a "limited free" assessment of evidence, in the sense that, on the one hand, the court is not constrained by external conditions in its assessment of evidence and, on the other hand, the court is bound by the requirements of the legislation. In this regard, Mr Bukovsky, a legal scholar, has articulated the following: "On the one hand, it does not restrict the judiciary in the assessment of evidence and, on the other hand, obliges the court to go into the substance of each piece of evidence in detail by comparing it with others and gives it the weight it deserves in terms of its internal value" [2].

In the contemporary digital age, electronic evidence has become an increasingly prominent aspect in both criminal and civil proceedings. This encompasses a wide range of digital data, including emails, text messages, social network records, metadata, files, and IP addresses, among others. However, the utilisation of this evidence poses a number of technical and legal challenges. These challenges pertain to the authenticity, integrity, and procedural requirements of the evidence, as well as the substantial complexity involved in assessing it.

The legal framework does not distinguish electronic evidence in civil proceedings as a specific category of evidence, nor does it define it as a separate legal institute, thus giving rise to questions regarding its assessment. We concur with the position espoused in the scientific literature that an equality mark cannot be affixed between the assessment of electronic evidence and the assessment of "paper" evidence [17]. Dr.iur. D. Ose also expressed a similar view with regard to electronic evidence in civil proceedings, stating that “the rules relating to the understanding and submission of written evidence no longer meet the needs of modern proceedings” [20].

The Criminal Procedure Law, conversely, has already recognised electronic evidence as a form of evidence since 2025, as outlined in Section 136 of the Law. This stipulates that evidence in criminal proceedings may encompass information on facts in the form of electronic information processed, stored or transmitted by automated data processing equipment or systems.

The necessity to enhance the legal framework is predicated on several factors, including the perceived absence of a legal definition in the Civil Procedure Act and the recognition that the creation, storage and handling of digital data may pertain not only to the alleged author of the data itself, but also to third parties who, in many cases, may not even be subject to the jurisdiction of the country in which the proceedings are taking place. For instance, if a photograph from a Facebook profile is submitted as evidence, but the defendant claims that his account was hacked and the photograph is fake or generated by artificial

intelligence, the court may encounter difficulties in determining its authenticity and admissibility as evidence. Researcher Juris Balodis-Boluge has highlighted the challenges posed by the absence of a definitive electronic evidence definition. Through a thorough evaluation of multiple court judgments, he has arrived at the conclusion that "in one criminal case, the court recognises data discs with communication control records as material evidence, in another criminal case the court recognises the evidence of a similar nature – a data disc with video control record – as an electronic document, but in another criminal case the court recognises such data discs as electronic evidence" [1]. The absence of a definition, in itself, would not pose a problem unless it resulted in a further negative impact on legal certainty due to the use of technology. The lack of regulation, i.e. technologies as such, does not have a single legal framework covering all areas and aspects. Instead, there is a multi-layered and fragmented framework that depends on the technology in question, its purpose and legal context. Legal regulation of technologies takes place at several levels: 1) At the international level, conventions, treaties and EU regulations that establish general guidelines. The international framework for electronic evidence is founded on several significant documents, including: the Budapest Convention on Cybercrime – the inaugural international document that established fundamental principles for the collection and exchange of electronic evidence among nations; and the EU Regulation on the European electronic evidence order [11] – which stipulates procedures for obtaining electronic evidence from providers of online services. from other EU countries; the General Data Protection Regulation (GDPR) – which regulates the processing of personal data and affects the storage and use of electronic evidence in judicial proceedings; 2) at regional level – for example, directives and regulations on data protection, artificial intelligence, cyber security, etc. are adopted at EU level. The EU Artificial Intelligence Act and the E-evidence Regulation [10] represent the primary legislative instruments in this regard. At the national level, each country establishes its own legal framework, which may align with international regulations but often exhibits significant variations. For instance, in the Republic of Latvia, the national framework for the utilisation of electronic evidence is encompassed within multiple legal acts: The Criminal Procedure Law stipulates the circumstances in which information obtained and utilised as electronic evidence in criminal proceedings is admissible. The Civil Procedure Law, while not explicitly providing for the use of electronic evidence, is relevant in this context as it establishes the framework for the administration of justice in the Republic of Latvia; despite the absence of explicit provisions in the Civil Procedure Law concerning the utilisation of electronic evidence in civil proceedings, the law does not inherently prohibit such practices. For instance, it permits the use of electronic evidence as a form of written evidence. However, the Personal Data Processing Act serves to complement the requirements stipulated in the GDPR, thereby imposing limitations on the processing of electronic evidence.

The basis for the assessment of electronic evidence consists of four well-established principles: 1) No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court; 2) In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions; 3) An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result; 4) The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to [13].

Whilst not seeking to question the necessity of the principles, it is important to note that their declaratory nature may be problematic in practice. There is a lack of standardised procedures, which hinders the collection and analysis of high-quality electronic evidence [19].

It is further noteworthy that the regulatory issues concerning electronic evidence are more pertinent to criminal proceedings. In contrast, civil proceedings, characterised by their adversarial nature, are driven by individual interests, which in practice renders the acquisition and verification of electronic evidence even more challenging. A significant challenge lies in the limited capacity for international cooperation. The legal framework for the taking of evidence abroad in civil matters is delineated by Regulation (EC) No 1206/2001 of the Council of the European Union of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil and commercial matters. The scientific literature has expressed the view that "one of the problems in practice is the identification of the lengthy and heavy-handed procedure in which the question in question (question of taking evidence — aut. note) is decided, i.e. Article 10 of Regulation (EC) No 1206/2001 provides that the requested court shall execute the request immediately or at the latest within 90 days of receipt of the request" [20].

It is important to note that the complexity of evaluating electronic evidence is not and cannot be decisive for its admissibility. The court's primary responsibility is to ensure the authenticity of electronic evidence, and consequently, its admissibility. Electronic evidence cannot be refused on the basis of its complex examination process. This assertion is supported by scientific literature, which acknowledges that electronic means of proof are analogous to traditional means and that electronic evidence does not constitute a novel form of evidence, but rather a novel technology-based verification mechanism for proof [12].

The EncroChat case [4] has become one of the most significant judgments in the European Union dealing with issues of electronic evidence collection, use and admissibility in criminal proceedings. This judgment underlines the need to clarify the boundaries between legitimate investigations and mass electronic surveillance. In the EncroChat case, law enforcement used digital infiltration to obtain encrypted communications that were

seen as evidence of criminal activity. However, the collection of such mass data, which also affects persons not involved in criminal activities, raised questions about respect for the right of individuals to privacy, as guaranteed by the Charter of Fundamental Rights of the EU and the European Convention on Human Rights, as well as about judicial supervision and control mechanisms necessary to prevent illegal or disproportionate behaviour by public authorities.

The CJEU emphasised that national courts must ensure that electronic evidence is obtained and used in accordance with EU and national law, particularly with respect to the fundamental right to privacy and to a fair trial. The Court underscored that the mass acquisition of electronic data, including the hacking of encrypted communication tools, is permissible only if it is carried out in accordance with the principles of proportionality and necessity, ensuring effective judicial control.

In the context of this Article, it is imperative to emphasise that one of the most salient issues in the EncroChat case was whether the data thus obtained may be the primary evidence in criminal proceedings. The Court observed that the procurement of evidence must be conducted in accordance with procedural regulations and the safeguarding of human rights; defendants must be capable of verifying the provenance and authenticity of the evidence, a task that can prove challenging in technically intricate cases; if the evidence is obtained unlawfully or infringes fundamental rights, it may be deemed inadmissible in court, particularly if it constitutes the sole or decisive basis of the accusation. These aspects assume particular significance given the use of EncroChat data in several European countries as pivotal evidence in the prosecution of criminal organisations.

The EncroChat case demonstrates significant legal and procedural challenges related to the acquisition and use of electronic evidence, emphasising the necessity for clear legal frameworks and legal oversight mechanisms to ensure fair legal action and privacy protection in the digital age. While laws and regulations establish principles for the use of electronic evidence, case law in this field is still developing in Latvia, highlighting the need for more detailed regulations regarding authentication, storage, and procedures for the use of evidence. The international exchange of electronic evidence frequently poses challenges related to the protection of jurisdiction and privacy, particularly when data is stored in foreign territories. These issues are set to become increasingly prevalent in national courts, as evidenced by the Norwegian Supreme Court's 28 March 2019 decision [22] concerning the conduct of searches at a company in relation to alleged computer fraud. The investigation involved a request for permission to conduct a search at the company's office in Oslo to access data stored on servers overseas that could provide information about the alleged fraud. The Supreme Court ruled that such a search did not violate the exclusive executive jurisdiction of other countries because the coercive measure was initiated in Norwegian territory against a Norwegian company with offices in Norway.

III. Technological Methods for Corroborating Electronic Evidence

The utilisation of electronic evidence within legal proceedings necessitates the employment of specialised methodologies, the purpose of which is to ensure its authenticity, integrity and legal admissibility. Digital forensics, a term not explicitly defined in legislation, is nevertheless regarded as a method in its own right. However, it is important to note that the content of digital forensics should be distinguished from the general norms of the Criminal Procedure Law regarding the procedures by which evidence is obtained and used, as well as the legal force of the Electronic Documents Law, which prescribes the use of electronic documents [7]. These legal provisions are of particular relevance in the context of digital forensics.

Digital forensics can thus be defined as a set of systematic methods and technologies used to identify, obtain, analyse and preserve electronic evidence while ensuring its integrity and admissibility in legal proceedings. It covers a wide range of processes, from data recovery to forensic analysis, and is used in both judicial investigations and cybersecurity incident analysis. Digital forensics is a branch of Forensic Science that focuses on the recovery and investigation of material found on digital devices in connection with cybercrime [5]. Digital forensics can thus be defined as a process aimed at identifying, obtaining, preserving and analysing electronic evidence, while ensuring that it remains consistent and that its use complies with legal norms. For digital evidence to be admissible in a court of law, it must meet a number of criteria, including authenticity, which means it reflects its original form; integrity, which ensures that any changes made can be tracked; compliance, which guarantees the importance of the evidence in a particular case; and permissibility, which determines that it has been obtained in accordance with the law.

Digital forensics employs a range of methods to ensure that these criteria are met, with disk imaging being of particular significance. This process involves the creation of an exact copy of the contents of a digital device using tools such as FTC Imager and dd. The process of data extraction allows for the retrieval of information from devices, including the restoration of deleted files. The analysis of network data using tools like Wireshark facilitates the identification of crucial evidence. Additionally, analysis of the file system and metadata is performed to determine the origin, change history, and other relevant details of documents and other electronic files.

Cryptographic methods, including hash functions such as MD5 and SHA-256, are also used to ensure the consistency and authenticity of electronic evidence, which allows one to check if data has been altered after it has been acquired. Digital signatures are used to authenticate documents and emails. Furthermore, the exploration of

communications and social networks, encompassing email and messaging analysis, the restoration of deleted posts, and the acquisition of information from social networks using open-source intelligence (OSINT) methods, is of paramount importance. The employment of OSINT methods facilitates the systematic search and analysis of identity-related information available on the Internet, thereby aiding in the identification of potential attack vectors and the implementation of preventive measures [23].

The utilisation of artificial intelligence has become increasingly pivotal in contemporary society, as automated data analysis methodologies facilitate the expeditious and precise identification of significant trends and anomalies. Artificial intelligence algorithms find application in domains such as facial and object recognition, a field of particular importance in the realm of digital forensics, encompassing image and video material.

A plethora of standards have been developed to ensure the security of data. Notable among these are: 1) Global Guidelines for Digital Forensics laboratories [15], which offers detailed guidelines for the establishment and operation of digital forensic laboratories covering topics such as staff qualifications, ethical standards, laboratory infrastructure and quality control procedures. The objective is to assist laboratories globally in developing standardised procedures for the procurement and examination of digital evidence that is admissible in court; 2) Best Practice Manual for the Forensic Examination of Digital Technology [9]. This manual provides guidance on best practices for the forensic examination of digital technologies. It includes guidelines on the taking, analysis and preservation of evidence and stresses the need for standardised methods and procedures to ensure the integrity and credibility of evidence in judicial proceedings; 3) the ISO/IEC STANDARD 21037 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence [14] is a set of guidelines for the identification, collection, acquisition and preservation of digital evidence. The purpose of the Standard is to assist organisations and professionals in ensuring that digital evidence is processed in accordance with internationally accepted standards, thereby preserving its integrity and admissibility in a court of law.

Adherence to these documents is imperative for ensuring the processing of digital evidence is conducted professionally and in accordance with international standards, thereby contributing to the credibility and efficiency of the judicial process.

Notwithstanding the advancements in digital forensics, numerous challenges persist in guaranteeing the credibility of electronic evidence. A salient issue is the rapid evolution of technology, necessitating the development of novel analytical tools and methods. Jurisdictional challenges further complicate the acquisition of evidence, as it frequently falls outside the scope of national legal control. Scientific literature indicates potential issues in data interpretation. For example, a study conducted by Itiel Dror and Nina Sunde found that experts' observations can be influenced by the contextual information provided to them and that consistency between expert analyses is often low. The authors emphasized the need for quality assurance measures to mitigate these biases and improve the reliability of the digital forensics' process [6].

In order to enhance the credibility of digital evidence, it is imperative to harmonise legislation to circumvent interpretative ambiguities and divergent approaches across jurisdictions. However, it is crucial to acknowledge that the admissibility, relevance and reliability of the evidence, as well as the burden of proof, rests with the national legal systems concerned. The European Court of Human Rights [7] has repeatedly emphasised that it does not function as the fourth body to examine the rules on admissibility and exclusion of evidence.

The new legal instruments, namely (1) Regulation (EU) 2023/1543, which provides a legal framework under which a Member State authority may require a service provider operating in the EU to provide or retain electronic evidence, irrespective of the location of the data, European Union, 2023/1543, (applies from 18 August 2026); and (2) Directive (EU) 2023/1544 laying down rules on the appointment of specially designated authorities and legal representatives to service providers offering services in EU. These designated authorities are entrusted with the responsibility of adopting, enforcing and implementing orders pertaining to the procurement of electronic evidence within the context of criminal proceedings (European Union, 2023/1544). This directive had to be incorporated into the national legal frameworks by 18 February 2026. However, it is noteworthy that these authorities do not regulate the admissibility of evidence at the national level. The determination of admissibility of evidence rests exclusively with the national provisions of EU law, rather than those of European Union law.

The electronic evidence regulation is principally focused on facilitating more efficient and expeditious access to electronic evidence. This is based on the assumption of mutual trust between EU Member States and the presumption that fundamental rights are adequately protected. However, in practice, this trust is not always justified, particularly due to concerns regarding the rule of law in certain states, meaning that the existing safeguards may be insufficient. In circumstances where such trust is lacking, it is essential to implement stronger protections for fundamental rights, as emphasized in Shurson's article [24] .

The introduction of new technologies capable of more effectively analyzing and authenticating electronic evidence is also essential. International cooperation is of critical importance, as digital evidence is frequently stored across different legal jurisdictions, which can result in restricted access to that evidence. Digital forensics is an evolving field whose importance continues to grow due to the increasing integration of technology into both everyday life and legal processes. Consequently, in the future, there may be a necessity for more extensive deliberations on establishing uniform admissibility criteria at the European

Union level as a whole. This perspective is also endorsed by G. Lasagni [25].

In conclusion, this chapter suggests that the development of the legal framework on electronic evidence within the European Union reflects a continuing balance between improving the efficiency of criminal proceedings and safeguarding fundamental rights. Despite the fact that the newly developed legal instruments have been demonstrated to enhance cross-border access to electronic evidence, questions of admissibility remain largely within the jurisdiction of national legal systems. This has the potential to result in divergent approaches in practice. In this context, greater coherence in evidentiary standards and procedural safeguards may become an important topic for future discussion in order to strengthen legal certainty and the effective protection of rights across the European Union.

IV. Conclusions

The utilization of electronic evidence in legal proceedings holds considerable promise for enhancing the efficiency and effectiveness of justice in the digital era. At the same time, it reveals a range of structural, legal and technical challenges arising from the interaction between rapidly evolving technologies and existing legal frameworks. This article has examined the current regulation of electronic evidence, its degree of alignment with technological realities, and the principal difficulties encountered in practice. These include issues related to mutual trust between Member States, divergences in national approaches, technical challenges concerning the collection, preservation, authentication and interoperability of electronic evidence, as well as legal and procedural constraints linked to jurisdiction, data protection requirements and the safeguarding of fundamental rights. Collectively, these challenges affect legal certainty, procedural efficiency and the consistent application of justice across the European Union.

Future developments may therefore require a more coherent and technologically informed approach to electronic evidence, combining legal harmonization with enhanced technical capabilities. This includes the adoption of tools capable of ensuring the authenticity, integrity and traceability of digital data, alongside greater interoperability between competent authorities. Given the inherently cross-border nature of electronic evidence, stronger cooperation at both the EU and international levels remains essential. The continued evolution of this field will likely depend on the ability to reconcile technological developments with effective procedural safeguards and a more uniform protection of fundamental rights throughout the European legal order.

While recent EU instruments seek to facilitate cross-border access to electronic evidence and improve procedural cooperation, their effectiveness continues to rely significantly on the principle of mutual trust between Member States. However, practical experience demonstrates that mutual trust cannot always be presumed, particularly in the context of ongoing concerns regarding the rule of law in certain jurisdictions. Consequently, the successful functioning of the electronic evidence framework depends not only on legislative harmonization at the EU level but also on the consistent implementation and enforcement of procedural safeguards at the national level, ensuring the effective and uniform application of common standards across Member States.

References

[1] J. Balodis-Bolužs, "Elektroniskā pierādījuma identitātes saturiskais definējums," Juridiskā zinātne, vol. 77, pp. 13–25, 2019. [Online]. Available: https://doi.org/10.22364/juzk.77.13.

[2] V. Bukovskis, Civīlprocesa mācības grāmata, Rīga: autora izdevums, 1933.

[3] Civilprocesa likums, Latvijas Republikas likums, Latvijas Vēstnesis, 326/330, 03.11.1998. [Online]. Available: https://likumi.lv/ta/id/50500-civilprocesa-likums .

[4] Court of Justice of the European Union, "Judgment in Case C-670/22, M.N. (EncroChat)," ECLI:EU:C:2024:3723, 2024, April 30.

[5] EC-Council, "What is digital forensics?," EC-Council. [Online]. Available: What is Digital Forensics In Cybersecurity? Phases, Careers & Tools .

[6] I. Dror & N. Sunde, "A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making," Forensic Science International: Digital Investigation, vol. 36, pp. 200-210, 2021. [Online]. Available: A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making - ScienceDirect

[7] Elektronisko dokumentu likums, Latvijas Republikas likums, Latvijas Vēstnesis, 169, 20.11.2002. [Online]. Available: Elektronisko dokumentu likums

[8] European Court of Human Rights, "Khan v. the United Kingdom [Judgment]," European Court of Human Rights, February, 2014.

[9] European Network of Forensic Science Institutes (ENFSI), Best practice manual for the forensic examination of digital technology, ENFSI, January 24, 2024.

[10] European Union, "Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for gathering electronic evidence in criminal proceedings," Official Journal of the European Union, 2023. [Online]. Available: Directive - 2023/1544 - EN - EUR-Lex.

[11] European Union, "Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings," Official Journal of the European Union, 2023. [Online]. Available: Regulation - 2023/1543 - EN - EUR-Lex

[12] D. Gorgieva, E. Gjorgioska, & Z. Stoileva, "Electronic evidence in civil proceedings," International Journal of Social Sciences and Humanities, vol. 28, pp. 1-21, 2021. [Online]. Available: ELECTRONIC EVIDENCE IN CIVIL PROCEEDINGS | Horizons - International Scientific Journal

[13] G. Horsman, "ACPO principles for digital evidence: Time for an update?," Forensic Science International Reports, vol. 100076, 2020. [Online]. Available: ACPO principles for digital evidence: Time for an update? - ScienceDirect

[14] International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence, ISO, 2012. [Online]. Available: ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

[15] INTERPOL, Global guidelines for digital forensics laboratories, INTERPOL, May 2019. [Online]. Available: https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf.

[16] Kriminālprocesa likums, Latvijas Republikas likums, Latvijas Vēstnesis, 74, 11.05.2005. [Online]. Available: Kriminālprocesa likums

[17] M. Krūmiņš, "Elektronisko pierādījumu vērtēšanas līkloči," Starptautisko un Eiropas Savienības tiesību piemērošana nacionālajās tiesās, pp. 312–318, 2020. [Online]. Available: juzk.78.33-Krumins.pdf

[18] Latvijas Republikas Senāts, "Krimināllietu departamenta 2018. gada 22. augusta lēmums lietā Nr. 11250014115, SKK-297/2018," ECLI:LV:AT:2018:0822.11250014115.2.L, 2018.

[19] M. K. Nickson, V. R. Kebande, H. S. Venter, & K.-K. R. Choo, "On the importance of standardising the process of generating digital forensic reports," Forensic Science International: Reports, vol. 1, 100008, 2019. [Online]. Available: On the importance of standardising the process of generating digital forensic reports - ScienceDirect

[20] D. Ose, "Elektroniskā saziņa kā rakstveida pierādījums civillietā," Juridiskā zinātne, vol. 78, pp. 32-33, 2022. [Online]. Available: juzk.78.03-Ose.pdf.

[21] Pierādījums, Britannica. [Online]. Available: Evidence | Definition, Law, Types, Examples, & Facts | Britannica

[22] Supreme Court of Norway, "HR-2019-610-A [Order]," Supreme Court of Norway, 2019. [Online]. Available: hr-2019-610-a.pdf

[23] M. Walkow, & D. Pöhn, "Systematically searching for identity-related information in the internet with OSINT tools," arXiv preprint, arXiv:2407.16251, 2024. [Online]. Available: [2407.16251] Systematically Searching for Identity-Related Information in the Internet with OSINT Tools

[24] J. Shurson, "The balance of efficiency and fundamental rights in the EU e-Evidence Regulation," New Journal of European Criminal Law, vol. 16, no. 3, 2025, doi: 10.1177/20322844251357090.

[25] G. Lasagni, "Admissibility of digital evidence," in The Cambridge Handbook of Digital Evidence in Criminal Investigations, V. Franssen and S. Tosza, Eds., Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2025, pp. 126–152.