TPM Vol. 32, No. S2, 2025
ISSN: 1972-6325
https://www.tpmap.org/

DIGITAL EVIDENCE IN COMPARATIVE CRIMINAL PROCEDURE: INTERNATIONAL EXPERIENCE AND THE PRACTICE OF JUDICIAL REVIEW

INHA KALANCHA
BORYS GRINCHENKO KYIV METROPOLITAN UNIVERSITY, KYIV, UKRAINE
ORCID: 0000-0002-5246-7337

VALERII BOZHYK
STATE TAX UNIVERSITY, IRPIN, UKRAINE
ORCID: 0000-0003-3162-0125

OLEKSII MUZYCHENKO
BORYS GRINCHENKO KYIV METROPOLITAN UNIVERSITY, KYIV, UKRAINE
ORCID: 0000-0002-0420-0646

VIKTOR VATSIYK
EDUCATIONAL AND SCIENTIFIC INSTITUTE OF LAW / PRINCE VLADIMIR THE GREAT INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT, KYIV, UKRAINE
ORCID: 0000-0001-8705-6223

Abstract: The article examines the international experience of using electronic evidence in the criminal procedures of the United States, the United Kingdom, France, Germany, at the supranational level of the European Union, and in Ukraine, focusing in particular on its impact on the mechanisms of judicial review. A comparative analysis is conducted of how different jurisdictions regulate the collection, preservation, authentication, and use of electronic evidence, alongside an overview of case law concerning the review of decisions based on newly discovered digital materials. The study identifies both commonalities and divergences in national approaches, which are presented in a comparative table of core legal provisions on electronic evidence. Special attention is given to the legal conflict between the U.S. CLOUD Act and the European General Data Protection Regulation, including the positions taken by the European Commission and national regulatory authorities. The conclusions provide practical recommendations for incorporating the most effective elements of international practice into the criminal procedure legislation of Ukraine.

Keywords: Criminal proceedings; Digital evidence; Criminal procedure; Hashing; Cybercrime; Evidence examination; Review of court decisions; Court decision.

INTRODUCTION

The modern digital era has profoundly transformed the nature of evidentiary processes in criminal proceedings. Electronic evidence - defined as any information in digital form that is relevant to a criminal case - has become increasingly significant in the practice of law enforcement agencies and courts. According to expert estimates, digital (electronic) evidence plays a role in approximately 90% of criminal cases. This trend is largely driven by the widespread use of digital technologies in everyday life, which has resulted in criminal traces increasingly manifesting in the form of electronic data, such as surveillance camera recordings, mobile phone data, computer files, electronic correspondence, and information from the Internet. At the same time, the use of electronic evidence presents new challenges to the justice system, raising a range of issues both at the stage of trial in courts of first instance and during appellate or cassation review of judicial decisions.

Electronic data, by their very nature, are intangible, easily copied, altered, or destroyed, and dependent on technical means for their storage and reproduction. It is essential to maintain a proper chain of custody - i.e., thorough documentation of who, when, and how the electronic evidence was collected, stored, and analyzed - in order to ensure its integrity and reliability during court proceedings. Furthermore, digital evidence frequently has a cross-border character, as data may be stored on servers located in other jurisdictions, which gives rise to jurisdictional conflicts and legal discrepancies, such as those stemming

from the incompatibility between the U.S. CLOUD Act and the European Union's General Data Protection Regulation (GDPR), as discussed below.

The stage of judicial review plays a pivotal role in ensuring legality and fairness within criminal justice systems, as it serves as an institutional safeguard against judicial errors and violations of human rights. Within this context, electronic evidence assumes particular importance, with its reliability, admissibility, relevance, and sufficiency being critical for delivering well-reasoned and just decisions. International judicial practice demonstrates that failure to comply with procedural standards or technical requirements during the collection, preservation, or assessment of digital information often results in such evidence being declared inadmissible, which, in turn, serves as grounds for the annulment of verdicts or a substantive review of decisions. Accordingly, the effectiveness of the judicial review stage largely depends on the quality of electronic evidence and adherence to proper procedures in its use (Bachmaier Winter & Queralt, 2018).

At the same time, international experience reveals considerable variability in approaches to judicial review in cases involving digital evidence. In jurisdictions based on common law systems (notably the United States, Canada, and the United Kingdom), the review process is shaped not only by formal procedural violations but also by more flexible assessments of evidentiary value, particularly from the standpoint of protecting the rights of the accused. In contrast, in civil law countries (including most EU member states and Ukraine), judicial review tends to be more strictly confined to compliance with procedural norms and formal rules of evidence (Angelenyuk, 2023).

Despite the relevance of the topic, scholarly literature has yet to develop sufficient methodological frameworks for comparative analysis of judicial review practices in cases where electronic evidence plays a key role. Therefore, there is a need not only to identify differences across national judicial practices but also to establish a conceptual foundation for harmonizing domestic approaches with international standards of justice.

Justice systems require tools to navigate the complexities of working with electronic evidence without infringing upon human rights. As such, the effective use of digital evidence represents both a vital resource and an essential instrument in the digital era. Nevertheless, the processing of electronic evidence presents distinct challenges: the lack of visual observation of information, the transitory and vulnerable nature of data, and the necessity of ensuring its accuracy and authenticity.

In light of the above, the aim of this study is to provide a comprehensive overview of international experience in the legal regulation and application of electronic evidence in criminal proceedings, to identify prevailing trends and challenges, with particular attention to methodological foundations for judicial review practices, and to formulate recommendations for legal regulation in this domain within Ukraine. To achieve this goal, the study analyzes the experience of the United States, the United Kingdom, France, Germany, the European Union, and Ukraine.

METHODOLOGY

To achieve the research objective, a comprehensive interdisciplinary methodology is applied, encompassing legal, comparative legal, and doctrinal approaches. The legal method enables the analysis of national legislation and international documents concerning Digital Evidence. The comparative legal method is employed to identify differences and commonalities in the regulation of digital evidence in the legal systems of the United States, France, the United Kingdom, Germany, the European Union, and Ukraine. The doctrinal analysis facilitates the systematization of scholarly views published in peer-reviewed Scopus/Web of Science journals, allowing for a critical assessment of existing approaches.

RESULTS AND DISCUSSION

The Budapest Convention on Cybercrime (ETS No. 185) establishes the core instruments for the collection of Digital Evidence, including the preservation of computer data, the provision of preserved data, the interception of traffic and content data, as well as the search and seizure of computer systems and storage media. These procedures must be carried out in accordance with proper procedural safeguards. States are required to align their national legislation with these principles. The Convention also provides mechanisms for cross-border cooperation in accessing digital evidence, including mutual legal assistance, extradition, and expedited cooperation through a 24/7 contact network.

Parties to the Convention are obligated to empower investigative authorities with the necessary rights to identify and seize computer data. Mechanisms for extradition and the preservation/transfer of Digital Evidence are also provided. For instance, Article 16 requires prompt preservation of computer data, while Article 18 establishes the obligation to provide mutual assistance to other member states in urgent cases involving the risk of data loss. Specifically, Article 18(1)(b) allows a service provider offering services within a country to be subject to an order, even if it is headquartered abroad. Furthermore, Article 32 permits access

to data stored in another country without requiring a formal request, provided the data is either publicly available or accessible with the user's consent.

The Second Additional Protocol to the Convention on Cybercrime (2022), focusing on enhanced cooperation and the disclosure of Digital Evidence, introduces new provisions related to: direct access by law enforcement to service providers located outside their jurisdiction; procedures for authentication and the protection of personal data; and security standards for cross-border access to information.

However, for universal implementation among EU Member States, a coordinated transnational doctrine is essential to ensure a balance between evidence accessibility and human rights protections. This includes the establishment of proper legality verification mechanisms (judicial oversight, independent audits), transparency of intergovernmental agreements - especially in terms of compatibility with the GDPR - and the integration of GDPR/ECHR standards into national legislation as part of protocol ratification.

Thus, while the Second Protocol marks a significant advancement in cyber law enforcement, its practical impact will depend on achieving a balance between the efficiency of law enforcement actions and the safeguarding of fundamental rights, which must be enshrined in domestic legal systems.

Ukraine has been a party to the Budapest Convention since 2006, which enables the formation of a modern criminal procedure model in the field of cybersecurity. The implementation of the Second Protocol is particularly relevant in the context of martial law and the necessity to document cybercrimes associated with the full-scale military aggression by the Russian Federation against Ukraine.

The European Union also places significant emphasis on regulating Digital Evidence, as it aims to establish a common area of security and justice. It actively implements supranational instruments to obtain and utilize Digital Evidence in criminal cases across its Member States. The most notable achievement in this area is the “e-evidence package,” adopted in 2023. This package comprises two interrelated legal acts: Regulation (EU) 2023/1543, concerning European production and preservation orders for Digital Evidence in criminal proceedings, and Directive (EU) 2023/1544, which obliges service providers offering services in the EU - but not established therein - to appoint a legal representative within the EU to receive such orders. These instruments establish a new European system for managing Digital Evidence.

The Regulation introduces a new tool - the European Production Order, which allows competent authorities in one Member State to request specific electronic data (such as content, traffic, or subscriber data) from service providers, including foreign companies operating in the EU via representatives. This order applies directly, without the need for Mutual Legal Assistance Treaties (MLATs) or other lengthy procedures. Providers are required to respond within a short deadline (10 days, or 8 hours in urgent cases). A second tool - the European Preservation Order - obliges the provider to immediately preserve existing data to prevent its deletion before competent authorities submit a formal request for access.

Importantly, the Regulation contains several safeguards for rights protection: an order cannot demand data that is subject to special protections (such as data relating to journalists); the executing state may refuse to recognize the order if it clearly violates fundamental rights; and for content data, the involvement of a judicial authority from the issuing country is required.

The precursor to the Regulation was Directive 2014/41/EU on the European Investigation Order (EIO), which entered into force in 2017. The EIO is a mutual recognition instrument that allows one EU country to task another with conducting a specific investigative measure (including the collection of Digital Evidence) (Covington & Burling LLP, 2019). However, the EIO still relied on the cooperation of authorities in the receiving country. In contrast, the new e-evidence Regulation directly targets cooperation with private companies (i.e., service providers). This shift reflects the EU’s recognition that crucial data is often held not by states, but by transnational corporations (such as social media platforms). The e-evidence package is thus a significant step in overcoming the limitations of traditional legal assistance frameworks, which are too slow for the digital age.

Despite introducing its own mechanism, the EU acknowledges that Digital Evidence frequently has a global character. Therefore, work is simultaneously underway on international agreements. First, the Second Additional Protocol (2022) to the Budapest Convention on Cybercrime, already discussed, is open for signature by countries outside the Council of Europe. The protocol provides new mechanisms for direct cooperation with internet service providers from foreign jurisdictions - similar to the European Regulation, but at the global level. The EU and most of its Member States have signed the Protocol and are preparing for its ratification, which will allow the exchange of Digital Evidence with countries such as the United States, the United Kingdom, Canada, and others on a multilateral basis.

Secondly, in 2019, the European Commission received a mandate to negotiate an EU–US agreement on Digital Evidence. These negotiations formally began in 2019, were paused to allow for alignment with internal EU legislation, and resumed in March 2023. The purpose of this agreement is to ensure mutual recognition of data access requests between the United States and the EU, thereby eliminating legal conflicts (for example, enabling U.S. companies to comply with European orders without violating U.S. law, and vice versa). As of 2025, negotiations are ongoing. Notably, two countries that were formerly or are closely affiliated with the EU (the UK, which is no longer a Member State, and Australia) have independently

concluded bilateral agreements with the U.S. under the CLOUD Act - namely the UK in 2019 and Australia in 2021. However, no such agreement yet exists between the EU and the U.S., and the Commission's initiative aims to close this gap.

A particularly sensitive area at the EU level concerns the conflict between law enforcement requirements and personal data protection. The General Data Protection Regulation (GDPR), in Article 48, explicitly states that the transfer of personal data in response to a request by a law enforcement authority of a third country is permitted only on the basis of an international agreement (e.g., a mutual legal assistance treaty). This provision is designed to protect EU residents from arbitrary disclosure of their data to foreign authorities. However, it complicates cooperation on Digital Evidence with countries such as the United States, which seek direct access to data through domestic laws (such as the CLOUD Act). As a result, the EU is working to develop common mechanisms that ensure European legal requests can be fulfilled without violating the GDPR.

One such solution is the requirement that every non-EU provider must appoint a legal representative within the EU - thus treating the request as internal for GDPR purposes. Another solution is the aforementioned negotiation of international agreements, which would serve as the “legal basis” demanded by Article 48 of the GDPR.

In conclusion, supranational regulation within the EU now defines the framework within which Member States harmonize their approaches to obtaining Digital Evidence. While the material rules for the admissibility of evidence in court remain governed by national laws, instruments such as European orders are designed to streamline and accelerate the collection of digital evidence in cross-border cases.

In the European Union, the problem of mutual recognition of Digital Evidence among Member States is addressed through mechanisms of international legal assistance and modern tools such as the European Production Order. Thus, Digital Evidence has become an integral part of the contemporary criminal process but requires special attention to the procedures for its collection, verification, and use.

Next, we examine how these issues are addressed in various jurisdictions, whose legislation and practices may serve as examples for Ukraine.

UNITED KINGDOM

The legal system of the United Kingdom does not codify the concept of “Digital Evidence” separately - digital data is treated by the courts as a type of evidentiary material (documents or physical evidence) and is subject to the general rules of evidence under English law. The key legislative act regulating police powers in evidence collection is the Police and Criminal Evidence Act 1984 (PACE) and its associated procedures. During the 1990s, British law included a specific requirement for computer records (Section 69 of PACE required proof of the proper functioning of a computer for its records to be admissible as evidence), but this provision was repealed in 1999 as outdated. Today, electronic documents and records are accepted as evidence on general grounds, though issues may arise regarding their authenticity or whether they constitute hearsay (e.g., automatically generated messages without a human author).

It is worth noting that the UK has specific legislation on communications interception and access to data from service providers. Primarily, this includes the Regulation of Investigatory Powers Act 2000 (RIPA), later replaced by the Investigatory Powers Act 2016 (IPA), which comprehensively regulates electronic surveillance, covert data extraction, and obligations of telecommunications companies to provide access to information. Although these laws primarily concern intelligence gathering and surveillance, they establish the legal framework within which digital evidence may be obtained for criminal proceedings. For instance, UK law permits disclosure orders for decryption keys or the extraction of data from devices by court warrant to enable investigators to access password- or encryption-protected evidence.

British courts have developed extensive case law on the use of Digital Evidence in a wide range of cases - from cybercrime to traditional crimes where key evidence includes CCTV footage, SMS messages, geolocation data from phones, and more. The English law of evidence relies heavily on the discretion of the judge concerning admissibility: the judge decides whether the authenticity of the digital record has been sufficiently demonstrated and whether its use would infringe on the rights of the accused. For example, in murder or robbery cases, video footage from surveillance cameras is often presented; if the defense challenges the authenticity of the footage, the prosecution must provide a witness or expert to explain how the footage was obtained and why it should be considered unaltered.

In the field of cybercrime, a number of cases highlight situations where UK courts have dealt with evidence collected abroad or supplied by foreign internet companies. Prior to 2020, such cooperation generally took place via Mutual Legal Assistance Treaties (MLAT). However, following the UK–US CLOUD Act agreement (2020), the process of obtaining Digital Evidence from American providers has significantly accelerated. For example, in terrorism investigations, British authorities may submit direct data requests to U.S.-based social media companies under agreed procedures, thereby bypassing the lengthy MLAT process.

UK courts have already considered cases involving such rapidly obtained data and are gradually developing standards for assessing their admissibility.

The United Kingdom is also known for its ACPO Guidelines on Digital Evidence, originally developed by the Association of Chief Police Officers (ACPO) in 2007. The latest version (5.0) was released in 2011–2012 and outlined four key principles for handling Digital Evidence, including the aforementioned requirement that data integrity must be preserved. Other principles require that all actions involving digital media be carried out only by trained personnel; that all actions during data access be logged (audit trail); and that responsibility for compliance with the law lies with the senior officer overseeing the investigation. These principles formed the basis of police and expert training in the UK. Although ACPO has since been reorganized (its functions transferred to the National Police Chiefs' Council, NPCC), the guidelines remain relevant and are often cited in court as best practice.In addition, the UK operates under the authority of the Forensic Science Regulator, who issues mandatory codes of practice for forensic laboratories. In 2017, the Regulator released a dedicated Digital Forensics Code of Practice, setting standards for laboratories analyzing computers, mobile phones, and other digital devices. This includes requirements for tool calibration, method validation, and staff competence. These measures are intended to ensure that digital evidence presented in court is reliable and collected in accordance with the highest standards.

FRANCE

France is a civil law country, and its rules on criminal procedure are codified in the Code of Criminal Procedure (Code de procédure pénale, CPP). Although French law does not provide a direct definition of "Digital Evidence," the legislator has established several specific tools for acquiring digital data. To combat crimes involving information technologies, provisions on "computer surveillance" were introduced: Article 706-102-1 of the CPP allows investigative authorities to covertly intercept computer data (e.g., installing keyloggers or spyware) upon judicial authorization in serious criminal cases.

Other provisions (Articles 706-95-1 and 706-95-2 CPP) govern orders to provide stored data, allowing investigative judges to compel service providers to disclose emails, messages, and other records in their possession. For real-time interception of content (such as reading incoming emails as they are received), traditional wiretapping rules (Articles 100 et seq. of the CPP) apply by analogy with telephone surveillance. In this way, French law integrates digital communication channels into existing investigative mechanisms (searches, seizures, wiretaps), while complementing them with specific provisions for cyberspace.

In 2016, France also revised its legislation, granting investigators broad powers in the field of digital investigations during states of emergency and counter-terrorism operations, French law enforcement agencies have been granted extended powers to collect Digital Evidence. For example, remote scanning of computers across networks, the use of IMSI-catchers (devices for intercepting mobile traffic), and other tools that effectively provide access to electronic data without the owner's knowledge have been authorized. These measures sparked debate over the balance between investigative efficiency and the right to privacy. However, the French Constitutional Council upheld their constitutionality, provided judicial oversight is in place.

French courts traditionally adhere to the principle of freedom of evidence in criminal cases - meaning the court may consider any type of evidence, provided it was obtained legally and is reliable. Digital Evidence is no exception. For instance, courts have accepted printouts of emails, SMS messages, GPS tracking data, and similar materials. A key challenge is the authentication of electronic documents: can a simple printout of an email be deemed reliable? French judicial practice generally requires corroboration - either through the testimony of the sender or recipient, or by presenting technical evidence (e.g., email headers containing metadata). In civil proceedings, France already recognizes electronic signatures, equating a properly signed email with a paper document. In criminal proceedings, however, the emphasis is not on formalities but on judicial discretion - the judge evaluates whether the file appears authentic and credible.

In recent years, French law enforcement has actively used digital evidence in investigations of terrorism and organized crime. A prominent example is the EncroChat operation carried out by the French Gendarmerie in 2020, in which they successfully hacked an encrypted communication network used by criminal organizations. As a result, millions of encrypted messages were obtained and used as evidence in hundreds of criminal proceedings across Europe (including Germany, the Netherlands, and France). French courts ruled that the evidence was obtained lawfully, as the operation was conducted on French territory with judicial authorization, and the resulting data was transferred to other countries through formal mutual legal assistance procedures. This case underscored the importance of international cooperation and data sharing in criminal matters.

Like other EU countries, France follows Council of Europe and Europol recommendations on the handling of Digital Evidence. Police and gendarmerie officers follow strict protocols for seizing digital devices - how to package and store them to maintain integrity. A national unit, C3N (Centrale Cyber de la Gendarmerie), specializes in cybercrime investigations and provides methodological guidance to investigators. France is a party to the Budapest Convention on Cybercrime, and has implemented key provisions into national law,

including Article 29 on expedited data preservation and other cooperation mechanisms. At the EU level, France has also adopted the European Investigation Order (Directive 2014/41/EU), which facilitates recognition and execution of evidence requests in digital format between EU Member States.

GERMANY

Germany's criminal procedure has specific features stemming from the principles of continental law and strong constitutional guarantees. The German legal system does not define "digital evidence" as a distinct category; instead, all types of evidence - including electronic - are subject to the principle of free evaluation of evidence by the court (Grundsatz der freien Beweiswürdigung) under the Code of Criminal Procedure (Strafprozessordnung, StPO). Judges are empowered to determine the credibility of evidence based on their internal conviction and the law. However, the process of evidence collection is strictly regulated: the StPO provides a comprehensive list of permissible investigative actions. If a certain method is not explicitly authorized by law, its use may render the evidence inadmissible. As a result, German legislation is gradually being updated to accommodate technological developments (Miller, 2023).

A key example is the inclusion of provisions on online interception and remote computer searches in the StPO. In 2008, the Federal Constitutional Court of Germany, in its landmark ruling on online searches (the North Rhine–Westphalia case), recognized a new fundamental right - the right to confidentiality and integrity of IT systems. The Court held that covert state access to an individual's computer constitutes a grave interference with privacy and is only permissible under very limited circumstances (such as threats to life or national security) and with strict procedural safeguards (judicial warrant, oversight mechanisms). Following this decision, the legislature introduced §100b StPO, allowing for covert remote searches of IT systems (Quellen-TKÜ and Online-Durchsuchung) under defined conditions. Additionally, §100a StPO was updated to regulate the interception of telecommunications, including internet-based communication. As a result, German investigators may now legally collect digital evidence from computers or networks - but only in serious cases and under strict judicial control (e.g., terrorism investigations).

In Germany, the admissibility of Digital Evidence is closely linked to the protection of constitutional rights. If evidence is obtained in violation of the right to privacy or without proper authorization, the defense may invoke the doctrine of Verwertungsverbote (prohibition on the use of illegally obtained evidence). Courts may exclude evidence obtained in clear breach of the law - for example, if police accessed a phone without a warrant. These matters are often reviewed by the Federal Court of Justice (Bundesgerichtshof, BGH) or even the Federal Constitutional Court. Following the introduction of §§100a/100b StPO, numerous cases have emerged in which defense attorneys have challenged the constitutionality of surveillance measures. So far, these provisions remain in effect, but courts consistently emphasize the need for strict compliance with the statutory conditions.

Regarding the authentication of Digital Evidence, the German approach is less formalistic than that of common law systems. There is no direct equivalent to the rules of "self-authentication"; instead, courts assess reliability on a case-by-case basis. For instance, metadata, chain-of-custody records, or expert opinions may be used to demonstrate that digital files have not been altered. The emphasis lies not in the formal structure of the document, but in whether the evidence appears credible and trustworthy to the judge.

In cases where the authenticity of digital evidence is disputed, the German court may order an expert examination or investigate the matter during a hearing. For example, in a case involving exchanged electronic messages, the court may summon an IT expert to explain whether the messages could have been falsified or question the individuals allegedly involved in the communication. Although Germany does not have a formal presumption regarding the reliability of computer systems (as the UK once did), in practice, courts assume the integrity of digital records unless there is reason to doubt the system's functionality. In other words, the burden of proving falsification typically lies with the party asserting it.

Germany, as a federal state, does not have a single national policing body like the UK's former ACPO. Instead, digital forensics guidelines are developed by the Federal Criminal Police Office (Bundeskriminalamt, BKA) and the State Criminal Police Offices (Landeskriminalämter, LKA). European standards also play a crucial role - particularly those issued by the European Network of Forensic Science Institutes (ENFSI), which maintains a dedicated working group on digital evidence and has published general guiding principles. Domestically, Germany has invested heavily in institutional capacity: thousands of IT specialists have been hired in law enforcement agencies, and modern forensic laboratories have been established. By the early 2020s, there were estimated to be around 11,000 digital forensic labs across the country. Nevertheless, the sheer volume of seized devices has led to backlogs in forensic analysis.

Thus, Germany emphasizes institutional preparedness in handling Digital Evidence - by training personnel, equipping labs, and developing methodologies - while incrementally adapting its legal framework to meet technological challenges and ensure compliance with constitutional requirements.

UNITED STATES

The United States does not have a unified code devoted solely to Digital Evidence, but several federal laws and regulatory frameworks govern various aspects of handling digital information in criminal proceedings. General admissibility standards - including those for digital evidence - are set forth in the Federal Rules of Evidence (FRE) (Robins Kaplan LLP, 2019). In 2017, amendments were introduced to simplify the use of Digital Evidence: Rules 902(13) and 902(14) allow certain records from electronic devices to be admitted based on a written certification by a qualified expert, eliminating the need for in-court testimony. Additionally, Rules 901 and 902 contain general provisions for authentication, which apply to digital materials - such as emails, social media posts, and computer records. Authentication can be established through provider confirmation or circumstantial evidence.

To obtain electronic information during criminal investigations, U.S. law enforcement relies on several statutes that regulate access to data stored by communication providers and online services. Chief among these are the Electronic Communications Privacy Act (ECPA) and its component, the Stored Communications Act (SCA). These laws establish procedures for accessing the content of electronic communications, metadata, and related information via judicial warrants, subpoenas, and formal requests depending on the type of information. In 2018, the U.S. Congress passed the CLOUD Act (Clarifying Lawful Overseas Use of Data Act), which explicitly authorized U.S. law enforcement to access data stored abroad - such as data held by American tech companies on servers located in Europe - provided a valid judicial warrant is issued. The law also simplified the process of concluding international agreements on access to Digital Evidence.

The adoption of the CLOUD Act was a direct response to increasingly complex legal disputes over extraterritorial access to data, particularly the case Microsoft Corp. v. United States. In that case, Microsoft refused to turn over email content stored on servers in Ireland, arguing that the Stored Communications Act lacked extraterritorial applicability. Before the U.S. Supreme Court could issue a decision, Congress passed the CLOUD Act as part of a broader legislative package (Perault & Salgado, 2024). This case was pivotal in the evolution of U.S. digital law, highlighting the limitations of jurisdiction in the absence of explicit rules on cross-border data access.

The CLOUD Act introduced significant changes to U.S. law by allowing authorities to demand Digital Evidence not only from servers located within the United States but also from those abroad - provided the company “possesses, controls, or has custody” of the data (Lawfare, 2022). Access is contingent upon a valid warrant issued by a U.S. judge based on probable cause in the context of a criminal investigation.

Over the past decades, U.S. courts have developed a substantial body of jurisprudence on Digital Evidence - both in terms of admissibility and the legality of collection methods. One of the leading precedents is the U.S. Supreme Court ruling in Riley v. California (2014), in which the Court unanimously held that police must generally obtain a warrant to search the contents of a cell phone seized during an arrest. The Court recognized that the volume and sensitivity of personal data stored on smartphones merit enhanced protection under the Fourth Amendment - on par with the protections granted to one’s home. This decision marked a milestone in the development of privacy doctrine in the digital age and significantly impacted investigative practices: law enforcement must now anticipate the need for warrants when accessing phones, computers, and other digital devices.

Another important area of case law concerns the authentication and reliability of digital evidence. Courts require the party submitting, for example, an email printout or screenshot of a webpage to establish its credibility - through witness testimony (e.g., from the recipient) or technical documentation indicating the origin of the data. In the Lorraine v. Markel (2007) decision (U.S. District Court), the court provided a detailed analysis of the criteria for admitting various types of Digital Evidence under the Federal Rules of Evidence The court in Lorraine v. Markel (2007) emphasized the key evidentiary principles applicable to electronic materials - authentication, hearsay, relevance, and integrity - and noted that the same standards apply to both electronic and traditional evidence, though their practical application may differ due to technical nuances. U.S. courts have also developed methods for identifying hidden metadata (e.g., creation or modification timestamps) and determining its evidentiary value. Expert witnesses in digital forensics often play a vital role in extracting and analyzing such data.

Numerous law enforcement guidelines have been issued in the United States regarding the handling of digital evidence. National standards are published by the Department of Justice (2023) and its agencies, such as the FBI's Computer Forensics Handbook. Professional bodies, including the Scientific Working Group on Digital Evidence (SWGDE), provide recommendations for the collection, preservation, and documentation of electronic materials. Additionally, the National Institute of Standards and Technology (NIST) releases reports and best practices for digital forensic techniques and tools. Although these documents are not legally binding, they function as de facto standards and are frequently referenced in court when evaluating the legality and reliability of investigative actions involving Digital Evidence.

One of the most critical legal conflicts related to the CLOUD Act concerns its compatibility with the EU's General Data Protection Regulation (GDPR). According to the GDPR, the transfer of personal data outside the EU is permitted only if adequate legal safeguards are in place—such as international agreements or sufficient protective mechanisms (IAPP, 2019). The CLOUD Act requires U.S. providers (e.g., Microsoft, Google) under U.S. jurisdiction to disclose data upon lawful request, regardless of where the data is physically stored. In contrast, the GDPR (Regulation (EU) 2016/679) mandates that such transfers may only occur to countries with an adequate level of protection, based on approved mechanisms (e.g., Standard Contractual Clauses, the now-invalidated Privacy Shield, or future replacements), or under limited exceptions as set out in Article 49. Notably, a simple foreign court order does not satisfy these conditions. Moreover, Article 48 of the GDPR explicitly states that any decision from a third-country court or authority requiring data disclosure will only be recognized if based on an international agreement (e.g., a mutual legal assistance treaty).

In 2019, the European Commission and Council issued a joint statement identifying negotiations with the U.S. on mutual access to Digital Evidence as a strategic priority and acknowledging the inevitability of legal conflicts in the absence of a formal agreement. The Commission adopted a pragmatic approach, recognizing the reality of the CLOUD Act while advocating for a bilateral treaty that would establish adequate safeguards and clear procedures. The aim is to ensure equivalent levels of data protection, such as requiring judicial oversight before U.S. authorities could request access to content relating to EU residents.

If U.S. authorities were to access data from the EU, they would be required to obtain judicial authorization from an EU court or notify the relevant European bodies. Ongoing negotiations are exploring a model similar to the U.S.–UK Agreement, but adapted to the supranational nature of the EU.

In July 2019, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) issued a joint legal analysis on the impact of the CLOUD Act. They concluded that the extraterritorial reach of U.S. law creates legal conflicts for European companies. According to the regulators, the only legitimate pathways for transferring data from the EU to the U.S. in the context of criminal investigations are mutual legal assistance mechanisms (MLATs) or a dedicated international agreement. Direct data requests from U.S. agencies should be rejected based on Article 48 of the GDPR, and such requests should be redirected through MLAT procedures.

The EDPB and EDPS (2019) also analyzed whether exceptions under Article 49 of the GDPR - such as the data subject's consent or public interest grounds - could apply. They concluded that such exceptions must remain narrowly interpreted and cannot serve as a legal basis for systematic data sharing. Even when a company wishes to cooperate with U.S. authorities, it must still identify a valid legal basis under Article 6 GDPR - and "legitimate interest" does not qualify, as it would infringe on data subjects' rights.

Thus, European regulators have taken a firm position: no direct data transfers without an international agreement. As a result, several companies - especially European ones - have adopted a cautious approach to U.S. requests. For example, some German providers publicly announced plans to encrypt data in such a way that it cannot be surrendered under the CLOUD Act or to relocate EU user data to European servers to avoid the applicability of U.S. law.

To resolve this conflict, in addition to a potential EU–U.S. agreement, legal reforms have been proposed. On the U.S. side, suggestions include amending the CLOUD Act to provide greater safeguards (e.g., requiring notification to the foreign data subject before disclosure or adhering to the originating country's laws). On the EU side, some experts proposed amending Article 48 GDPR to allow transfers in clearly defined cases involving democratic partner countries. However, as of now, no such amendments have been enacted.

Another potential solution is the expansion of multilateral treaties: once the Second Additional Protocol to the Budapest Convention enters into force in multiple jurisdictions, requests under its provisions could be considered "agreed international procedures," thus mitigating legal conflicts.

Ukraine, in recent years, has begun reforming its criminal procedure legislation to address the challenges of the digital age. However, the legal framework governing Digital Evidence remains underdeveloped. The country is moving toward harmonization with European standards: it has signed (but not yet ratified) the Second Additional Protocol to the Budapest Convention, is strengthening cooperation with Eurojust and Europol regarding digital evidence exchange, and is considering the implementation of EU recommendations implementation of rules similar to the European Production Order may also become relevant in the event that Ukraine attains EU membership. Thus, despite current shortcomings, there is a growing awareness of the need for reform and gradual progress in that direction.

COMPARATIVE ANALYSIS: KEY PROVISIONS ON DIGITAL EVIDENCE

For clarity, we summarize the main characteristics of legal regimes on Digital Evidence in the jurisdictions examined in Table 1 below.

TABLE 1 COMPARISON OF APPROACHES TO DIGITAL EVIDENCE IN SELECTED JURISDICTIONS

Criterion	USA	United Kingdom	France	Germany	EU (supranational)
Definition of 'Digital Evidence' in law	Not separately defined; electronic records are subject to general rules of evidence.	Not specifically defined; electronic materials are treated as documents or physical evidence depending on context	No specific definition; law describes data categories (content, traffic, etc.) through access instruments	Not expressly defined; the StPO does not use the term 'digital evidence'; general evidentiary principles apply	Regulation 2023/1543 provides a description of electronic data covered by European orders (content, traffic, subscriber).
Admissibility and authentication	Special rules: FRE 902(13)-(14) allow self-authentication of data copies with certification; courts require confirmation of authenticity (via witnesses or experts) for social media, email, etc.	No formal requirements, judge decides case-by-case; notarized web pages accepted in civil cases, flexible approach in criminal ones. ACPO emphasizes data integrity	Freedom of evidence principle: accepted if court deems it credible; e-signatures recognized (in civil cases); in criminal proceedings, a copy suffices if no doubt exists	Free judicial evaluation of evidence; no presumption of authenticity, but if uncontested, digital records are admitted. In case of dispute – expert examination is appointed	Regulation requires data to be lawfully obtained and verified; admissibility is determined by national courts, though data received under the Regulation must be accepted
Legal instruments for data collection	ECPA/SCA: warrants, subpoenas to providers (email, cloud); PATRIOT Act expanded powers post-2001; CLOUD Act (2018) enables access to data abroad via international agreements	PACE 1984 – general search/seizure powers; IPA 2016 – interception regimes, provider obligations to store/disclose data; CLOUD Act agreement with US for expedited access.	CPP: Articles 706-95, 706-102 etc. – production of electronic data, interception of emails equated to wiretaps. Budapest Convention: data preservation, international cooperation	StPO: §100a (telecom interception), §100b (online search of computers) – introduced for serious crimes since 2017; provider data access regulated by Telecommunications Act and constitutional court rulings on data protection	Regulation 2023: European production and preservation orders (direct provider requests via national authorities, short deadlines); Directive – provider representatives in EU to receive orders. EIO Directive 2014 – mutual legal assistance
Judicial/ constitutional oversight	Extensive case law: warrant required for device	Judicial control of investigative actions: warrant	French Constitutional Council approves counter-	Federal Constitutional Court: 2008 ruling on IT-Grundrecht (limits on online	CJEU rulings on data retention (Digital Rights Ireland 2014,

	searches (Riley v. California); surveillance limits (Carpenter v. US – location data needs warrant); exclusionary rules apply to evidence obtained in violation of the Fourth Amendment	required to search private devices. Human rights case law includes ECtHR ruling in Barbulescu v. Romania (email monitoring at work, influencing UK practice)	terrorism laws with reservations; Court of Cassation recognizes data copies if procedure is followed. Courts generally admit new evidence methods if judge-approved	searches); 2020 ruling on cybercrime (proportionality required for mass data collection). BGH allows use of foreign intelligence data (e.g., EncroChat case)	Privacy International 2020) limit national laws – blanket retention violates privacy rights; evidence obtained under mass retention can be excluded under EU law
Standards and best practices	NIST, DOJ Guidelines, SWGDE – technical standards; cyber training in each agency; significant role of private experts and consultants	ACPO Guide (4 principles); Forensic Regulator's Codes; cyber investigation training (College of Policing); cooperation with Europol EC3	National Gendarmerie instructions; participation in EU projects (Paris LEA platform); own investigative software (e.g., Brigades numériques). CoE recommendations adopted (e.g., Digital Evidence Guide training)	ENFSI and EU lab standards; BKA issues "Merkblätter" guidance for police; regular IT-evidence training in police academies; US-Germany joint training exchanges	Eurojust and Europol issue manuals (e.g., Manual on Digital Evidence for Prosecutors); EVIDENCE2e-CODEX project – cross-border exchange platform; joint investigation teams focusing on cybercrime

Notes. The table provides a concise overview; actual legal regulation is more nuanced and dynamic.

As can be seen, all jurisdictions face similar challenges in handling digital evidence, yet they address them in different ways. In some countries (e.g., the U.S., the UK), case law and flexible standards play a central role; in others (e.g., France, Germany), detailed legislative regulation under the supervision of constitutional authorities prevails; while at the EU level, new supranational mechanisms are being created.

Thus, approaches to the evaluation and use of electronic evidence in the context of judicial review vary significantly across jurisdictions, resulting in the heterogeneity of procedural standards and the level of guarantees for protecting the rights of participants in criminal proceedings. In particular:

In the legal systems of countries adhering to the Anglo-American legal tradition (e.g., the United States, the United Kingdom, Canada), there is a high degree of specificity regarding the requirements for the authenticity and admissibility of electronic evidence. In most cases, failures to comply with rules on the storage or transmission of electronic information lead to the reversal of decisions at the appellate or cassation level. Landmark cases such as R. v. Bailey (UK) and United States v. Ganias (US) illustrate the critical importance of ensuring that electronic evidence complies with constitutional standards, including the right to privacy and protection against unreasonable searches and seizures.

In civil law jurisdictions (such as France and Germany), there is a discernible trend towards institutionalizing procedural filters in the evaluation of digital evidence at the review stage. However, their application remains fragmented and is often contingent on established national judicial practices. In certain cases, courts prioritize a formal assessment of procedural validity over considerations of digital integrity or the risk of data tampering.

In European Union jurisdictions, there is a gradual emergence of supranational standards governing the handling of electronic evidence in criminal proceedings, particularly in light of the implementation of Regulation (EU) 2023/1543 and Directive (EU) 2023/1544. An analysis of the case law of the Court of Justice of the European Union reveals a growing tendency toward harmonizing approaches to the admissibility of electronic evidence, especially in cross-border contexts. Nevertheless, the review of judicial decisions on such grounds remains largely subject to the discretion of national courts.

Ukraine, despite formally recognizing electronic evidence under Article 99-1 of the Criminal Procedure Code, has yet to develop a coherent doctrine for its assessment at the appellate or cassation stages. Judicial practice reveals inconsistencies, with some cases demonstrating unconditional acceptance of electronic evidence without proper verification, while others reflect unwarranted disregard of such evidence. This inconsistency poses risks to the principles of adversarial proceedings and the right to a fair trial.

Thus, the findings of this study demonstrate that the effectiveness of using electronic evidence in the process of judicial review is directly dependent on the following factors:

- the existence of clearly defined admissibility criteria;
- a harmonized approach to the technical and procedural aspects of data handling;
- the institutional capacity of courts to properly assess digital materials in accordance with human rights standards.

The absence of adequate normative and judicial regulation regarding the treatment of electronic evidence at the stage of judicial review constitutes a significant source of legal uncertainty. This underscores the need for both the unification and improvement of procedural safeguards in this area.

RECOMMENDATIONS FOR IMPLEMENTING INTERNATIONAL EXPERIENCE IN UKRAINE

An analysis of foreign experience allows us to identify several elements that should be introduced to improve Ukraine's criminal procedure in the context of Digital Evidence:

1. Legal definition of Digital Evidence. It is necessary to introduce a clear definition of "Digital Evidence" into the Criminal Procedure Code of Ukraine as a separate source of evidence, specifying its scope. This could be modeled after international documents—for instance, as any information in digital form, lawfully obtained and suitable to establish facts relevant to the crime. The procedural format for submitting such evidence (e.g., a digital storage medium, a certified printout with an electronic signature) and the procedure for verifying its authenticity should also be defined.

2. Procedures for ensuring integrity and admissibility. Laws or by-laws should establish requirements for handling electronic media: documenting the seizure, hashing (i.e., calculating a checksum) during copying to confirm data integrity (as recommended by Kalancha and Stolitnii (2019), Kalancha and Harkusha (2021), and drafting a detailed inspection protocol for digital content. While such practices are already applied by some investigators, they require standardization. Moreover, the use of expert certificates of authenticity should be permitted - for example, an expert could certify that a copy is identical to the original, which would suffice for court purposes (in the absence of objections) without necessitating the expert's in-person testimony in every case.

3. Guidelines and training for law enforcement. Ukrainian law enforcement agencies should develop an official Guide on Digital Evidence Handling, incorporating best practices (potentially through translation and adaptation of the UK's ACPO Guide and the Council of Europe's manual). This document should be distributed to every investigator and operative officer, and its principles integrated into training curricula. Key principles - data immutability, documentation of each step, use of forensic copies that do not affect the original, and secure storage of original data - must become part of professional standards.

4. International cooperation and legal mechanisms. Ukraine should ratify and implement the Second Additional Protocol to the Budapest Convention, which will greatly simplify the process of obtaining Digital Evidence from abroad - especially from companies that are not subject to traditional treaties. It is also advisable to establish direct cooperation with service providers: for example, by signing memoranda of understanding with major IT companies regarding prompt responses to requests from Ukrainian law enforcement agencies, within legal limits. In the context of European integration, Ukraine should begin preparing for future participation in the EU e-evidence system - analyzing in advance what legislative changes would be necessary to both execute e-evidence requests from EU Member States and issue its own.

5. Protection of human rights in the digital space. When borrowing foreign experience, it is essential not only to expand investigative powers, but also to ensure adequate safeguards. Ukraine should explicitly require that access to personal devices or online accounts is allowed only by court order and only in serious criminal cases, following the German model. It is also necessary to regulate how to protect the confidentiality of third-party data inadvertently obtained during digital evidence collection (e.g., if a phone contains private photos unrelated to the crime). A filtering procedure should be introduced: for example, in the United States, "taint teams" or independent experts are used to separate irrelevant private data before law enforcement accesses device content.

Implementing these recommendations would make the practice of handling Digital Evidence in Ukraine more predictable, effective, and aligned with international standards**.** Especially in the context of Ukraine's EU integration**,** harmonization in this area is an essential element of justice sector reform.

CONCLUSION

The conducted research has demonstrated that electronic evidence plays a central role in the modern criminal process, particularly at the stage of judicial review, where such evidence can either reinforce the positions of the parties or cast doubt on the legality of a rendered verdict. Based on a comparative analysis of practices in the United States, the United Kingdom, EU member states, and Ukraine, the following key conclusions can be drawn:

1. The development of flexible and technologically adaptive procedural standards. In the United States, the approach to electronic evidence has evolved through updates to the Federal Rules of Evidence and the development of case law that seeks to strike a balance between the right to privacy and the needs of justice. Similarly, the United Kingdom combines traditional judicial discretion with professional guidelines (e.g., those issued by the Association of Chief Police Officers and the Forensic Science Regulator), thereby ensuring both flexibility and predictability in judicial practice.
2. Normative integration of electronic evidence in civil law systems. In countries such as France and Germany, electronic evidence has been incorporated into national legislation through amendments to their criminal procedure codes, which now explicitly regulate the use of instruments such as production orders and online searches. These measures are accompanied by constitutional oversight mechanisms, serving as practical examples of legal proportionality in action.
3. Harmonization at the European Union level. The EU has made a significant leap forward by introducing the e-evidence regulatory package, which establishes a unified legal framework for obtaining data from service providers in cross-border criminal cases. Particular emphasis is placed on aligning these rules with third-country legal systems (for example, mitigating conflicts between the GDPR and the U.S. CLOUD Act), thereby laying the groundwork for a model of global legal integration.
4. Institutional Challenges and Potential in Ukraine. Despite the formal recognition of electronic evidence in the Criminal Procedure Code of Ukraine (Article 99-1), national practice remains fragmented and requires comprehensive reform. The absence of secondary legislation and unified standards for the collection, preservation, and verification of digital evidence hampers its effective use at the appellate and cassation stages. Moreover, a significant gap exists between domestic practice and the contemporary demands of cross-border cooperation in combating cybercrime.

   It is advisable to incorporate into Ukraine's legal system well-established formulations from international instruments - particularly Regulation (EU) 2023/1543 - and to enshrine procedural safeguards ensuring the authenticity, admissibility, and relevance of digital evidence. It is also essential to develop detailed procedural guidelines for handling electronic evidence, drawing on British professional standards and European practices rooted in the principle of proportionality.

A balance must be maintained between procedural efficiency and the protection of fundamental rights, avoiding excessive interference with privacy. This can be achieved by relying on the case law of the U.S. and EU courts, where judicial oversight acts as a crucial safeguard of individual rights. Ukrainian law enforcement and judicial authorities must be fully integrated into international mechanisms for the exchange of electronic evidence, taking into account both technical and legal requirements of the digital age.

Thus, electronic evidence holds the potential to become a robust and reliable instrument within the criminal justice system. However, its effectiveness is directly contingent upon the quality of legal regulation, judicial practice, and the legal system's ability to adapt to digital realities. Implementing the proposed measures would not only enhance trust in judicial decisions but also promote the harmonization of Ukraine's criminal procedure with European and international standards in the domain of digital evidence.

REFERENCES

1. ACPO (2012). Good Practice Guide for Digital Evidence, Association of Chief Police Officers (Version 5.0).
2. Angelenyuk, A.-M. Y. (2023). The use of Digital Evidence in the criminal procedural law of Ukraine (problematic issues). Scientific Bulletin of Uzhhorod National University. Law Series, (79, Part 2), 214–218.
3. Bachmaier Winter, L., & Queralt, J. (Eds.). (2018). Cambridge Handbook of Digital Evidence. Commentary on German law and the absence of a legal concept of "digital evidence".
4. Council of Europe (2022). Digital Evidence Guide (Version 3.0) – emphasizes chain of custody and authenticity of digital evidence.
5. Covington & Burling LLP (2019). European Data Protection Board Issues Opinion on U.S. CLOUD Act. Inside Privacy Blog, July 23, 2019.
6. EDPB & EDPS (2019). Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 12 July 2019.

7. Kalancha, I. H., & Harkusha, A. M. (2021). Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects. Juridical Scientific and Electronic Journal, 8, 336–339. https://doi.org/10.32782/2524-0374/2021-8/77
8. Kalancha, I., & Stolitnii, A. (2019). Formation of the Institute of Digital Evidence in the Criminal Process of Ukraine. Problems of Legality, 146, 179. https://doi.org/10.21564/2414-990x.146.171218
9. Lawfare (2022). Navigating Toward an EU–U.S. Agreement on Digital Evidence, Lawfare Blog (discussing CLOUD Act agreements with UK, Australia).
10. Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. Forensic Science International: Digital Investigation, 45, 301492. https://doi.org/10.1016/j.fsidi.2023.301492
11. Riley v. California, 573 U.S. 373 (2014). U.S. Supreme Court decision (June 25, 2014), holding that warrantless search of a cell phone during arrest is unconstitutional.
12. Robins Kaplan LLP (2019). What's Happening? The Impact of FRE 902(14) on eDiscovery. Real Talk Business Law Update (Winter 2019).
13. U.S. Department of Justice & European Commission (2023). Joint Press Release: Resumption of U.S.–EU Negotiations on Digital Evidence, March 2, 2023.