DOI: 10.38146/bsz-ajia.2026.v74.i10.pp2759-2787

Cross-border admissibility of electronic evidence in cybercrime investigations: Lessons from the European Union for Rwanda[1]

Nshimiyimana Francois Regis
cybercrime researcher specializing in electronic evidence
Károli Gáspár University of the Reformed Church in Hungary,
Doctoral School of Law and Political Sciences
regisnshimiye82@gmail.com

Abstract

Aim: This paper examines the cross-border challenges surrounding the admissibility of electronic evidence in cybercrime investigations, drawing insights from the European Union to inform Rwanda's legal and institutional development. It aims to determine how EU procedural safeguards and cross-border mechanisms can inform Rwanda's judicial response to cybercrime, particularly in relation to the admissibility and management of electronic evidence.

Methodology: The study employs a comparative legal research approach, focusing on Hungary, Germany, and Estonia as representative EU jurisdictions. Their selection reflects both legal and practical diversity within the EU while ensuring comparability with Rwanda's predominantly civil law system. Although Rwanda blends elements of civil and common law, its legal structure, rooted in Belgian and French civil law traditions, shares fundamental characteristics with these EU countries. The analysis draws on legislation, case law, academic literature, and institutional reports to assess normative and procedural approaches to electronic evidence and cross-border cooperation.

Findings: The research reveals that the EU jurisdictions studied have developed relatively advanced mechanisms for the authentication, preservation, and cross-border exchange of electronic evidence through frameworks such as the

[1] The manuscript was submitted in Hungarian. Received: 10. 03. 2026. Revised: 05. 04. 2026. Accepted: 21. 05. 2026.

Budapest Convention, its Second Additional Protocol, and the European Investigation Order. In contrast, Rwanda faces significant procedural and institutional challenges, including limited harmonization with international standards and inadequate technical capacity. The study underscores the need for clear procedural standards, institutional capacity-building, and targeted legislative reforms inspired by EU practices to ensure the reliability and admissibility of electronic evidence before Rwandan courts**.**
Value: This paper contributes to comparative legal scholarship by offering an evidence-based analysis of how civil law jurisdictions manage electronic evidence in cybercrime investigations. It provides actionable policy recommendations to help Rwanda modernize its evidentiary framework, enhance judicial cooperation, and align with evolving international norms in the field of cybercrime. The study ultimately underscores the centrality of electronic evidence to effective, fair, and technologically-responsive criminal justice systems.

Keywords: Electronic evidence, cybercrime, cross-border investigations, admissibility of evidence.

Introduction

The increasing reliance on digital technologies in modern society has fundamentally transformed the nature of criminal activity and criminal investigations (URL1). Cybercrime, by its very nature, frequently involves electronic data stored or transmitted across multiple jurisdictions, making electronic evidence a central element in the detection, prosecution, and adjudication of such offenses. Courts are therefore increasingly required to assess the admissibility, authenticity, and reliability of digital evidence obtained beyond national borders. This development raises complex questions of criminal procedure, international cooperation, and fundamental rights. Within the European Union, a relatively dense legal framework has emerged to regulate the cross-border collection and use of electronic evidence, notably through the Convention on Cybercrime of the Council of Europe (Budapest Convention), its Second Additional Protocol, and instruments such as the European Investigation Order. These mechanisms seek to reconcile the effectiveness of criminal investigations with the protection of privacy, due process, and judicial oversight. In contrast, jurisdictions outside the European Union, including Rwanda, face the challenge of integrating international standards on electronic evidence into domestic criminal procedure while responding to the growing transnationalization of cybercrime. Rwanda has adopted legislation on cybercrime and elec-

tronic evidence, but the practical application of these norms in cross-border investigations remains uncertain, particularly concerning issues such as authentication, chain of custody, and judicial control over foreign-sourced data. This article, therefore, examines how selected European Union member states: Germany, Estonia and Hungary, regulate the admissibility of electronic evidence in transnational cybercrime cases and considers what legal and institutional lessons may be drawn for Rwanda. By adopting a comparative legal approach, the study aims to identify procedural safeguards and cooperation mechanisms that could enhance the reliability, legality, and judicial acceptance of electronic evidence in Rwanda's criminal justice system.

Background

The rapid expansion of digital technologies has fundamentally transformed the nature of criminal investigations, making electronic evidence central to the prosecution of cybercrime. Electronic evidence includes data generated, stored, or transmitted through computers, mobile devices, digital networks, and online platforms, and it frequently constitutes the primary or exclusive form of proof in cyber-enabled offenses (Singla, 2025). As cybercrime continues to grow in scale and sophistication, the reliability, authenticity, and admissibility of digital data have become critical issues for criminal justice systems worldwide (Abdullah et al., 2025). Cybercrime is inherently transnational, as perpetrators, victims, and digital infrastructures are often located in different jurisdictions. This creates serious obstacles for law enforcement authorities, who must rely on international cooperation to secure electronic evidence stored abroad (Cerezo, Lopez & Patel, 2007). Courts, in turn, are required to assess whether such foreign-sourced digital evidence satisfies domestic procedural and evidentiary standards. To address these challenges, the Council of Europe adopted the Convention on Cybercrime (Budapest Convention), which establishes substantive cybercrime offenses and procedural mechanisms for the collection, preservation, and international exchange of electronic evidence (Council of Europe, 2001). These mechanisms have been further reinforced by the Second Additional Protocol, which facilitates cooperation with foreign service providers and the disclosure of electronic evidence in cross-border investigations (Council of Europe, 2023). Within the European Union, these international standards are complemented by regional instruments such as the European Investigation Order and emerging e-evidence rules, which seek to streamline cross-border access to electronic data while safeguarding fundamental rights (Juszczak & Sason, 2023). For Rwanda, these developments are particularly significant. Al-

though Rwanda has enacted legislation on cybercrime and electronic evidence, the increasing use of cloud services and foreign-based digital platforms means that national authorities depend ever more heavily on international cooperation to obtain critical digital evidence (Kabano & Habarurema, 2023). This situation raises important legal and institutional challenges concerning admissibility, judicial oversight, and the integrity of electronically stored data obtained from abroad.

The growing scale of cybercrime and its implications for evidence collection and criminal prosecution

Cybercrime continues to expand at an alarming rate, imposing significant economic, social, and legal challenges worldwide. In 2021, the global cost of cybercrime was estimated at approximately $6 trillion, with projections suggesting it could reach $10.5 trillion annually by 2025 (AllahRakha, 2024). Such economic losses have far-reaching impacts, affecting governments, businesses, and individuals alike.

The European Union has experienced a marked increase in cyber threats, with ransomware attacks rising by 150% between 2019 and 2021 (ENISA, 2021). These attacks have disrupted critical sectors, including healthcare, finance, and infrastructure, emphasizing the urgent need for robust cybersecurity measures. Phishing remains the most prevalent cyberattack vector, accounting for more than 90% of reported cyber incidents according to international cybersecurity assessments (URL2). Developing countries, including Rwanda, face an accelerated rise in cyber threats due to rapid digital adoption and limited cybersecurity infrastructure. The vulnerability of individuals and businesses in such contexts underscores the pressing need for enhanced legal and technical frameworks to prevent, investigate, and prosecute cybercrime. Cross-border cybercrime further compounds these challenges. In the past five years, international cybercrime cases have increased by 70%, creating significant obstacles for jurisdictional enforcement and the collection and admissibility of electronic evidence (URL3). These dynamics highlight the critical importance of harmonized legal approaches and international cooperation to ensure the effective prosecution of cybercrime across jurisdictions.

Problem statement

The cross-border collection and admissibility of electronic evidence have become one of the most complex issues in contemporary cybercrime investiga-

tions. While digital data is indispensable for identifying offenders and proving criminal conduct, its transnational nature creates difficulties related to jurisdiction, procedural legality, data protection, and evidentiary reliability (Casino et al., 2022). In Rwanda, electronic evidence is formally recognized under national cybercrime legislation, yet the procedural framework governing its collection, authentication, and use in court remains underdeveloped, particularly in cases involving foreign-based service providers. Law enforcement authorities face delays and legal uncertainty when seeking access to data stored abroad, while courts lack detailed statutory guidance on how to assess the integrity, chain of custody, and legal validity of such evidence (Kabano & Habarurema, 2023; Prosecution v. Nshimiyimana, 2013). Differences in data protection standards and the absence of comprehensive bilateral or multilateral cooperation mechanisms further complicate the admissibility of cross-border electronic evidence. Within the European Union, significant progress has been achieved through the Budapest Convention, the European Investigation Order and EU data protection and e-evidence initiatives. However, variations in national implementation and constitutional safeguards continue to affect how foreign-sourced electronic evidence is evaluated by domestic courts (Ferreira & Gromova, 2023). The central problem addressed by this research is how Rwanda can develop a coherent and legally robust framework for the admissibility of cross-border electronic evidence by drawing on the experience and best practices of European Union jurisdictions.

Methodology

This study employs a comparative legal research methodology to examine how different civil law jurisdictions regulate the collection, preservation, and admissibility of electronic evidence in cybercrime investigations. Germany, Estonia, and Hungary are selected as representative European Union Member States because they combine civil law traditions with advanced legal and institutional frameworks for handling digital evidence. Their systems provide a meaningful basis for comparison with Rwanda, whose criminal justice system is also primarily rooted in the civil law tradition.

The research is based on a doctrinal analysis of international treaties, European Union legislation, national laws, judicial decisions, and scholarly literature on cybercrime and digital evidence (Mifsud Bonnici, Tudorica & Cannataci, 2018; Ferreira & Gromova, 2023). Particular attention is given to procedural rules governing cross-border cooperation, forensic integrity, judicial authorization and the evaluation of electronic evidence in criminal proceed-

ings. By comparing these legal frameworks, the study identifies principles and practices that may be adapted to the Rwandan context in order to strengthen the reliability, legality and admissibility of electronic evidence in cybercrime cases.

Literature review and identified gaps

The proliferation of cybercrime has prompted extensive scholarly attention, particularly regarding the collection and admissibility of electronic evidence across borders. Electronic evidence, encompassing digital data, communications, and transactional records, has become a cornerstone for the investigation and prosecution of cyber-offenses (Ferreira & Gromova, 2023). However, its cross-border nature introduces complex legal, technical, and procedural challenges, including jurisdictional conflicts, inconsistencies in evidentiary standards, and difficulties in ensuring the integrity and authenticity of data (Casino et al., 2022). The European Union (EU) has established robust legal instruments and procedural mechanisms to address these challenges, offering valuable insights for comparative analysis. For instance, the Council of Europe's Convention on Cybercrime and its additional protocols provide structured frameworks for cross-border cooperation, the expedited exchange of electronic evidence, and enhanced judicial collaboration. Empirical studies highlight the effectiveness of these instruments in mitigating delays, reducing evidentiary disputes, and improving prosecutorial outcomes in Germany, Estonia, and Hungary, which, as civil law jurisdictions, share procedural similarities with Rwanda (Mifsud Bonnici et al., 2018; Ferreira & Gromova, 2023).

Despite these advancements, several gaps remain in the literature. First, there is limited research on the adaptability of EU mechanisms to jurisdictions in developing countries, where legal frameworks, technical infrastructure, and institutional capacities differ significantly from those in Europe (AllahRakha, 2024). Second, while the procedural aspects of cross-border evidence exchange are well-documented, fewer studies explore the practical challenges of admissibility and authentication of electronic evidence within domestic courts, particularly in mixed legal systems such as Rwanda's (Cerezo et al., 2007). Third, most existing analyses emphasize either doctrinal or technical perspectives but rarely integrate both, leaving a gap in understanding how legal theory and practical enforcement interact in complex cybercrime investigations (Casino et al., 2022; Ferreira & Gromova, 2023). This study addresses the need for research that integrates doctrinal legal analysis with empirical evidence, filling critical gaps in the understanding of electronic evidence in cybercrime investigations.

It provides actionable recommendations for Rwanda, drawing on best practices from Germany, Estonia, and Hungary, to improve the collection, authentication, and admissibility of electronic evidence. Implementing these practices can strengthen Rwanda's legal system while aligning it more closely with international standards for cross-border cooperation in combating cybercrime.

The concept of electronic evidence in cybercrime investigation

Electronic evidence is pivotal in identifying, prosecuting, and resolving criminal activities in cybercrime investigations. Electronic evidence refers to any data or information that is stored or transmitted in digital form and can be utilized in legal proceedings. This includes data from computers, mobile devices, cloud storage, and networks (Brown, 2015). The importance of electronic evidence has grown significantly as technology has advanced and become more integrated into daily life.

Definition and characteristics of electronic evidence

Electronic evidence, also commonly termed digital evidence, refers to any information that is created, stored, or transmitted in a digital format and is admissible in judicial proceedings. Its significance has grown markedly in the context of cybercrime, where digital interactions constitute both the medium and the target of criminal activity. Unlike traditional forms of evidence, electronic evidence possesses distinct attributes, including volatility, ease of alteration, and dependency on technological infrastructure, which present both challenges and opportunities for law enforcement, forensic investigators, and judicial authorities. Understanding these characteristics is essential for ensuring the reliability, authenticity, and admissibility of electronic evidence in court (Brown, 2015).

Nature and types of electronic evidence

Electronic evidence manifests in various forms, including but not limited to emails, metadata, digital logs, social media content, electronic documents, and multimedia files. Emails and instant messages often contain crucial information about communication patterns and intent, while metadata provides contextual details such as timestamps, geolocation data, and file history that can corroborate timelines (URL 4). Digital logs, including system and transaction logs, record user activities and can illustrate a sequence of events essential to reconstructing a crime scene (Wahl, 2023). Social media posts, videos and other

multimedia files also serve as valuable sources of information in establishing facts and linking suspects to criminal activity.

Volatility and authenticity issues

Electronic evidence is highly fragile and can be easily altered, deleted or damaged during collection, storage or transmission. Unlike physical evidence, changes to digital data may occur without leaving any visible trace, which makes it difficult to detect whether information has been modified or compromised (URL5). This vulnerability creates serious risks for the reliability of electronic evidence in criminal proceedings. To ensure that electronic evidence remains trustworthy, investigators must follow strict forensic procedures. These include preserving a clear chain of custody, documenting every action taken with the data, and using technical tools such as hash values to verify that the content has not been altered during handling or transfer (Narasimhan & Kala, 2024). Courts generally require such safeguards before accepting digital evidence, because only evidence that is proven to be authentic, intact and reliable can be admitted and relied upon in criminal trials.

Relevance of electronic evidence in cross-border cybercrime

The rapid expansion of digital technologies has significantly changed the way crimes are committed and investigated, particularly in the field of cybercrime (Hadjab, 2025). Criminals increasingly use online platforms, digital devices and communication networks to plan, commit and conceal offenses. As a result, electronic evidence has become essential for identifying suspects, reconstructing criminal activities and proving offenses in court. In cross-border cybercrime cases, electronic evidence plays an even more critical role. Data relating to a single offense may be stored on servers in different countries, processed by foreign service providers, and accessed through international networks. This means that law enforcement authorities must rely on legal and technical mechanisms that allow them to obtain, preserve and use digital evidence across national borders. The relevance of electronic evidence in this context can be understood through several key factors: the transnational nature of cybercrime, the development of EU legal instruments such as the e-Evidence package, the need for mutual trust between jurisdictions, the rules governing admissibility, and the practical difficulties involved in implementing these frameworks.

The nature of cybercrime and the cross-border challenge

Cybercrime is inherently transnational. Unlike traditional crimes, cyber offenses are committed through digital networks that operate without regard to territorial borders. A single cybercrime may involve an offender located in one country, a victim in another, and electronic evidence stored on servers in several different jurisdictions. This geographical fragmentation creates serious legal and procedural challenges for law enforcement authorities and courts. For example, in a phishing or online fraud case, a suspect operating from Rwanda may use an email service based in the United States, a cloud server located in Ireland, and a payment platform registered in the Netherlands. The evidence needed to identify the offender, such as IP addresses, login records, transaction logs and message content is therefore controlled by foreign service providers. Domestic authorities cannot lawfully access such data without relying on international cooperation mechanisms. These difficulties were clearly illustrated in the Microsoft Ireland case (United States v. Microsoft Corp., 2016), in which U.S. authorities sought access to emails stored on Microsoft servers located in Ireland. Microsoft refused to comply, arguing that U.S. warrants could not be enforced extraterritorially. Although the case was eventually resolved through new U.S. legislation (the CLOUD Act), it demonstrated how conflicts of jurisdiction can obstruct access to electronic evidence in cross-border investigations.

In Europe, similar challenges arise in cybercrime cases involving online platforms such as Google, Facebook or WhatsApp. When national authorities require subscriber data, content data or traffic data stored abroad, they must rely on legal frameworks such as the Budapest Convention on Cybercrime (ETS No. 185) and, within the EU, the European Investigation Order under Directive 2014/41/EU. Articles 16 to 21 of the Budapest Convention specifically regulate the expedited preservation and disclosure of stored computer data and traffic data, recognizing the risk that digital evidence may be quickly deleted or altered. However, even with these instruments, cross-border cybercrime investigations remain complex. Differences in national criminal procedure, data protection laws, and constitutional standards can delay or prevent the transfer of electronic evidence. For example, evidence lawfully collected in one state may be rejected in another if it does not meet domestic standards on judicial authorization or privacy protection. German courts, for instance, have excluded electronic evidence obtained through foreign surveillance measures that did not comply with the constitutional right to informational self-determination. These legal and practical obstacles show why cybercrime cannot be effectively

prosecuted without strong international cooperation and harmonized procedural rules. The cross-border nature of cybercrime therefore makes electronic evidence both indispensable and legally sensitive, requiring a careful balance between investigative efficiency, state sovereignty, and the protection of fundamental rights (URL6).

The EU e-Evidence Package as a response to the challenges of transnational digital evidence

In response to the challenges posed by cross-border cybercrime, the EU has developed the e-Evidence package, which seeks to streamline the process by which law enforcement authorities can access electronic evidence across Member States swiftly and legally. This legislative framework includes two key instruments, which are: The Regulation on European production and preservation orders and the Directive on the appointment of legal representatives for gathering electronic evidence (Wahl,2023). The e-Evidence package was introduced to address the increasing demand for cross-border access to digital data, with reports indicating that 85% of criminal investigations require such access and a significant portion of requests are directed at service providers located outside the requesting jurisdiction (Cami, 2024). In facilitating faster and more efficient data sharing processes, the package enhances law enforcement's capacity to combat transnational cybercrime while ensuring respect for privacy and fundamental rights.

Mutual trust as a foundation of EU legal frameworks on electronic evidence

The effective collection and use of electronic evidence in cross-border cybercrime investigations within the European Union depends fundamentally on the principle of mutual trust between Member States. This principle assumes that each Member State respects EU law, fundamental rights, and minimum procedural standards when conducting criminal investigations (Juszczak & Sason, 2023). On this basis, judicial authorities can recognize and execute requests for electronic evidence issued by authorities in other Member States without re-examining the merits of the underlying investigation. The EU e-evidence framework is built upon this mutual trust. It enables national authorities to request and receive electronic data across borders through streamlined procedures, reducing reliance on traditional mutual legal assistance and minimizing delays. When judicial authorities trust that their counterparts apply equiva-

lent safeguards for legality, proportionality, and data protection, electronic evidence can be exchanged more quickly and with greater legal certainty. Mutual trust also plays a decisive role in the admissibility of electronic evidence. If evidence is collected in compliance with EU standards in one Member State, it is more likely to be accepted by courts in another Member State, thereby reducing the risk that evidence will be excluded due to procedural irregularities (URL7). In this way, mutual trust not only facilitates cooperation but also strengthens the integrity and reliability of cross-border electronic evidence, which is essential for the effective investigation and prosecution of cybercrime.

Admissibility standards for electronic evidence

For electronic evidence to be used effectively in criminal proceedings, it must satisfy both legal and technical standards governing admissibility. Courts generally examine whether the data was obtained under lawful authority, whether it is authentic and intact, and whether it is relevant and reliable for establishing the facts of the case (Kerr, 2005). These requirements are designed to ensure that digital evidence is not only technically accurate but also legally obtained and procedurally fair. To support a consistent and structured assessment of these requirements, the Harmonized Model for Digital Evidence Admissibility Assessment (HM-DEAA) offers a comprehensive framework for evaluating the collection, preservation, and presentation of electronic evidence across different jurisdictions (Antwi-Boasiako & Venter, 2017). Compliance with such standards enhances the credibility of digital evidence and protects the procedural rights of the accused, thereby reinforcing confidence in the administration of justice in cybercrime cases.

Challenges in implementing EU cross-border electronic evidence frameworks

Despite the advancements brought by legislative measures like the e-Evidence package, several challenges remain in their implementation due to varying national laws on data privacy, differing judicial processes, and the need for harmonization across legal systems. Ensuring that digital evidence is collected and transferred in compliance with local and international legal standards requires ongoing cooperation among law enforcement agencies, judicial authorities, and private sector stakeholders. Continuous monitoring and dialogue are essential to address discrepancies in legal frameworks and to promote best practices for managing electronic evidence in cross-border investigations. In

the researcher's opinion, electronic evidence is indispensable for combating cross-border cybercrime, as it allows law enforcement agencies to collect and present crucial digital information efficiently and lawfully (URL8). The EU's e-Evidence frameworks, built on principles of mutual trust and respect for fundamental rights, offer valuable guidance for addressing the complexities of transnational cybercrime. However, this research argues that the effectiveness of such measures depends on continuous collaboration between states and strict adherence to admissibility standards, ensuring that electronic evidence remains a reliable and authoritative tool in the pursuit of justice.

Legal frameworks for admissibility of electronic evidence in EU.

The legal frameworks governing electronic evidence in the European Union (EU) are shaped by international conventions, EU directives, and national legislation, aiming to ensure effective cross-border cooperation while safeguarding fundamental rights (URL9). The Budapest Convention on Cybercrime, formally known as the Convention on Cybercrime of the Council of Europe (2001), is the principal international treaty governing crimes committed through computer systems and digital networks. It establishes a comprehensive legal framework for international cooperation in combating cybercrime and provides common standards for the collection, preservation and admissibility of electronic evidence in criminal proceedings. The Convention covers a wide range of cyber offenses, including illegal access to computer systems, data interference, system interference and the misuse of devices, as set out in Articles 2 to 7. These provisions create a harmonized substantive criminal law basis for prosecuting cybercrime across participating states. In addition to defining offenses, the Convention contains detailed procedural rules designed to enable effective cross-border investigations. Articles 16 to 21 regulate key investigative measures such as the expedited preservation of stored computer data, the disclosure of subscriber information, and the real-time collection of traffic data, which are particularly important in cases where electronic evidence may be quickly altered or deleted. The Convention has been further strengthened by its Additional Protocols. These address specific forms of cyber-related criminality, including child sexual exploitation and the dissemination of racist or xenophobic material, and introduce enhanced mechanisms for international cooperation and the disclosure of electronic evidence. In particular, the Second Additional Protocol (ETS No. 223) significantly improves the ability of authorities to obtain electronic evidence directly from foreign service providers and

to cooperate more efficiently in transnational investigations. Within the European Union, the Budapest Convention has served as a foundational model for the development of national cybercrime legislation. Germany has incorporated its principles into the *Strafgesetzbuch* and the *Strafprozessordnung*, particularly in relation to computer-related offences and the procedural handling of electronic evidence. Estonia has aligned its Penal Code and criminal procedure laws with the Convention, enabling more effective investigation and prosecution of cybercrime. Hungary has likewise integrated the Convention's standards into Act C of 2012 on the Criminal Code, ensuring that its domestic legal framework on electronic evidence and cybercrime is compatible with its international obligations.

EU directives and regulations on cross-border cooperation and electronic evidence

In addition to the Budapest Convention, the European Union has developed a set of binding legal instruments to facilitate cross-border access to electronic evidence while ensuring respect for fundamental rights and data protection. These instruments are designed to replace slow and fragmented mutual legal assistance procedures with more efficient and legally secure mechanisms (Juszczak & Sason, 2023; Eurojust, 2024). Directive 2014/41/EU on the European Investigation Order (EIO) introduced a uniform system through which judicial authorities in one Member State may request investigative measures, including the collection of electronic evidence, from another Member State in a legally binding manner (European Parliament and Council, 2014). The EIO has significantly accelerated cooperation in cybercrime investigations by allowing direct requests for subscriber data, traffic data, and other digital records. In practice, Germany makes extensive use of the EIO to obtain electronic communications data held by service providers in other EU countries, while Estonia relies on the same mechanism to support investigations into organized and technologically sophisticated cybercrime. Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) provides a harmonized framework governing the processing and transfer of personal data, including electronic evidence used in criminal proceedings (European Parliament and Council, 2016). Compliance with the GDPR ensures that digital evidence is obtained lawfully, proportionately, and in a manner that respects the right to privacy. In Germany, the Federal Commissioner for Data Protection and Freedom of Information oversee compliance with data protection standards during criminal investigations, while Estonia incorporates GDPR-based safeguards into its digital

forensics and secure data-exchange systems. The EU has further strengthened cross-border access to electronic evidence through the e-Evidence legislative package, which enables judicial authorities to request certain categories of data directly from service providers located in other Member States, subject to judicial oversight and fundamental rights safeguards (Eurojust, 2024). Regulation (EU) 2020/1783, although adopted primarily for civil and commercial matters, reflects the EU's broader commitment to modernizing and simplifying cross-border evidence gathering through digital means (European Parliament and Council, 2020). Hungary has aligned its criminal procedure rules with these EU developments, thereby improving its capacity to obtain electronic evidence efficiently in cross-border cybercrime investigations. Taken together, these EU directives and regulations complement the Budapest Convention by creating an integrated legal framework that enables faster, more reliable, and rights-compliant access to electronic evidence across national borders.

Standards of admissibility and reliability in EU courts

The admissibility of electronic evidence in courts across the European Union is governed by both national criminal procedure rules and overarching EU principles aimed at ensuring fairness, legal certainty, and the protection of fundamental rights. Although detailed rules vary between Member States, a number of common standards are applied throughout the EU (Kerr, 2005). First, relevance is required. Electronic evidence must be directly connected to the facts of the case and capable of assisting the court in determining criminal responsibility. German courts, for example, have excluded digital material that did not have a clear link to the legal issues in dispute, reflecting the strict application of relevance and proportionality principles (Noerr, 2023). Second, authenticity must be established. Courts must be satisfied that the electronic evidence is genuine and has not been altered. This is usually demonstrated through a documented chain of custody, time-stamped records or digital signatures. In Estonia, forensic experts play a central role in verifying the authenticity of electronic evidence in cybercrime cases, supported by the country's secure digital identity and e-signature infrastructure (e-Estonia, 2025). Third, integrity is essential. Digital data must remain unchanged from the moment it is collected until it is presented in court. Any alteration, whether intentional or accidental, may undermine its evidentiary value. In Hungary, investigators rely on specialized forensic tools and secure storage systems to preserve data integrity, particularly in cases involving encrypted communications (Narasimhan & Kala, 2024). Fourth, electronic evidence must be obtained in accordance with the

law, including EU rules on data protection. The General Data Protection Regulation (GDPR) requires that personal data be collected and processed lawfully, proportionately and for legitimate purposes. Evidence obtained in breach of these requirements may be excluded from criminal proceedings (European Parliament and Council, 2016). Finally, judicial discretion remains decisive. Judges assess whether electronic evidence satisfies the standards of relevance, authenticity, integrity, and legality. While German courts place strong emphasis on procedural safeguards and privacy rights, Estonian courts seek to balance efficient digital investigations with the protection of fundamental rights, and Hungarian courts focus on maintaining evidentiary reliability while facilitating effective cross-border cooperation (Szongoth, 2024). Overall, EU standards on electronic evidence are shaped by the Budapest Convention and EU legislation designed to enhance cross-border cooperation while safeguarding individual rights. The experiences of Germany, Estonia, and Hungary demonstrate both the benefits and the challenges of applying harmonised evidentiary standards in cybercrime cases.

Comparative analysis of EU approaches to electronic evidence

The management and admissibility of electronic evidence in criminal proceedings vary across EU Member States, reflecting differences in legal frameworks, institutional structures, and technological capacities (Mifsud Bonnici, Tudorica & Cannataci, 2018). Germany, Hungary, and Estonia exemplify these variations while also demonstrating the influence of EU instruments such as the European Investigation Order (EIO) and the e-Evidence regulation. Germany emphasizes procedural safeguards and data protection within a federal system, ensuring electronic evidence aligns with both national and EU standards. Hungary has centralized mechanisms that integrate mutual legal assistance and cross-border cooperation, though challenges persist in operationalizing EU instruments efficiently. Estonia, notable for its advanced digital governance, leverages technological innovation to facilitate secure authentication, transmission, and verification of electronic evidence. Comparing these jurisdictions provides insights into best practices, common challenges, and potential pathways for harmonizing digital evidence procedures across civil law systems.

The Hungarian system of electronic evidence

Hungary's legal framework for electronic evidence is primarily established under Act C of 2012 on the Criminal Code (Büntető Törvénykönyv, Btk), which

criminalizes a wide range of cyber offenses (URL10). Relevant provisions include Sections 422–424 Btk., which address illegal access to information systems, illegal system interference, data interference, and illegal interception of computer data. These provisions form the substantive legal basis for prosecuting cybercrimes involving digital or electronic evidence. Procedurally, the handling and admissibility of electronic evidence are governed by Act XC of 2017 on Criminal Proceedings (Be.), which outlines the investigative powers of authorities, the collection and preservation of electronic evidence, and the conditions under which such evidence may be introduced in court. Furthermore, Act XXXVIII of 1996 on International Mutual Legal Assistance in Criminal Matters facilitates cross-border judicial cooperation, allowing Hungarian authorities to request or provide assistance in obtaining electronic evidence from other jurisdictions in line with Mutual Legal Assistance Treaties (MLATs) and European Union mechanisms.

Institutionally, Hungary has developed robust structures to support international cooperation in cybercrime investigations. The Hungarian National Police (Nemzeti Nyomozó Iroda) actively cooperate with Europol, Eurojust, and Interpol, particularly through the European Cybercrime Centre (EC3) (Vas & Szongoth, 2024). Hungary is also a party to the Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence (2022), which together form the cornerstone of its international legal obligations. Despite these advancements, Hungary continues to face challenges in ensuring full harmonization between domestic procedural rules and evolving EU legislation, such as the forthcoming Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence. Divergences occasionally arise concerning the admissibility of electronic evidence obtained from foreign jurisdictions, particularly when procedural safeguards or data protection standards under Regulation (EU) 2016/679 (GDPR) are not uniformly applied. Addressing these gaps is essential for strengthening Hungary's role in European and international cybercrime enforcement (Szongoth, 2024).

The German legal framework for electronic evidence

Germany's system for dealing with electronic evidence is shaped by its federal legal structure, meaning that both the federal government and the Länder (states) play a role in criminal justice and data protection. The main criminal law governing cybercrime is the German Criminal Code (Strafgesetzbuch – StGB), which criminalises, among others, the illegal access to data, data in-

terception, data alteration, and computer sabotage (StGB, §§ 202a–202d; §§ 303a–303b). The collection and admissibility of electronic evidence are regulated primarily by the German Code of Criminal Procedure (Strafprozessordnung – StPO). Sections 94 to 100b StPO provide the legal basis for the seizure of digital devices, searches of data carriers, and the interception and monitoring of telecommunications (StPO, §§ 94–100b). These provisions allow investigators to access electronic data but only under strict judicial supervision and procedural safeguards. Germany has also aligned its national system with European Union law. In particular, the Act on the European Investigation Order in Criminal Matters (2017) implements Directive 2014/41/EU, which allows German authorities to request or provide electronic evidence to other EU Member States in a fast and legally secure manner (URL11). This is especially important in cybercrime cases, where data is often stored outside the country where the offense was committed. At the same time, the handling of digital evidence must comply with data protection and privacy rules. These are governed by the EU General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (Regulation (EU) 2016/679). These laws ensure that law enforcement authorities process electronic data lawfully, proportionately, and only for legitimate investigative purposes. German courts place strong emphasis on constitutional rights, especially the right to informational self-determination, which derives from Article 2(1) in conjunction with Article 1(1) of the basic law (Grundgesetz) (GG). The Federal Constitutional Court has ruled that intrusive digital investigative measures, such as online searches of computers, are only lawful if they are based on clear legal authority and include strong safeguards for fundamental rights (BVerfGE 115, 320 – *Online-Durchsuchung*). German courts also require that electronic evidence obtained from abroad must meet German procedural and human-rights standards to be admissible. Overall, the German framework seeks to balance the effective prosecution of cybercrime with strong constitutional, and data-protection guarantees, while also enabling cross-border cooperation within the EU.

Estonia: Legal and institutional framework for electronic evidence

Estonia stands out as a global leader in digital governance and the integration of technology in criminal justice processes. Its comprehensive digital identity infrastructure, established under the Identity Documents Act (2009) and the Digital Signatures Act (2000), enables citizens to authenticate themselves and sign documents electronically using secure national ID cards. This infras-

tructure supports the collection, authentication, and transmission of electronic evidence, facilitating both domestic investigations and international cooperation. The Penal Code (Karistusseadustik) and the Code of Criminal Procedure (Kriminaalmenetluse seadustik) provide the substantive and procedural bases for addressing cybercrimes and managing electronic evidence (URL12). Sections 206–217 of the Penal Code criminalize illegal access to information systems, interference with data or systems, and unauthorized use of telecommunications services. Procedurally, Sections 64–65 and 90–91 of the Code of Criminal Procedure regulate the seizure, preservation, and admissibility of electronic data, ensuring that digital evidence is handled under strict legal safeguards.

Estonia's framework aligns closely with European Union law and the Council of Europe's Convention on Cybercrime. The country has also ratified the Second Additional Protocol (2022), which enhances cross-border cooperation and the disclosure of electronic evidence. Furthermore, the Electronic Identification and Trust Services Regulation (EU) No. 910/2014 (eIDAS Regulation) underpins Estonia's system for secure electronic signatures and trust services, ensuring that digital documents and evidence are recognized as legally valid across EU jurisdictions.

Institutionally, Estonia cooperates through Europol's European Cybercrime Centre (EC3) and contributes to the SIRIUS project, sharing expertise on digital forensics and evidence exchange. The country's commitment to technological innovation and procedural transparency has positioned it as a model for digital justice systems worldwide, demonstrating how technological solutions can reinforce the rule of law and the effective prosecution of cybercrimes.

Comparative legal assessment of electronic evidence frameworks in Hungary, Germany and Estonia

The comparative analysis reveals both shared strengths and significant divergences among Hungary, Germany, and Estonia in managing electronic evidence in cybercrime investigations. All three jurisdictions have established comprehensive legal frameworks that criminalize cyber offenses and provide mechanisms for cross-border cooperation, largely reflecting their obligations under the Budapest Convention (ETS No. 185) and its Second Additional Protocol (2022). However, the degree of alignment and technological integration varies. Germany emphasizes procedural safeguards and fundamental rights protection, ensuring that electronic evidence collected domestically or abroad complies with constitutional and data protection standards under the

Basic Law and Regulation (EU) 2016/679 (GDPR). Hungary has achieved substantial harmonization with EU instruments such as Directive 2014/41/EU on the European Investigation Order, but practical challenges persist in ensuring the admissibility of evidence gathered through mutual legal assistance and in maintaining uniform data protection standards. Estonia, in contrast, represents a highly digitized model, where the implementation of the Electronic Identification and Trust Services Regulation (EU) No. 910/2014 (eIDAS Regulation) and nationwide digital identity infrastructure have transformed the authentication and transmission of electronic evidence.

For other civil law jurisdictions, the experiences of these three EU Member States offer valuable insights. Legal harmonization with EU standards must be accompanied by institutional modernization and technological innovation to strengthen investigative efficiency and judicial reliability. As Buçaj observes, balancing legal certainty with technological advancement remains essential to preserving both the integrity and the admissibility of electronic evidence in cross-border cybercrime investigations (Buçaj, 2024).

The Rwandan legal framework on electronic evidence

Rwanda's legal framework on electronic evidence and cybercrime has evolved in response to the increasing reliance on digital technology and the challenges posed by cyber-related offenses. The country has enacted specific laws and policies aimed at regulating electronic transactions, protecting data, and combating cybercrime. However, while these legal provisions are a step toward aligning with international standards, the implementation of these laws faces significant institutional and technical challenges.

Existing laws on electronic evidence and cybercrime

Rwanda has established a legal basis for the use and admissibility of electronic evidence in criminal investigations and court proceedings. The primary legislative instruments include the Law No. 24/2016 of 18/06/2016 governing information and communication technologies and the Law No. 60/2018 of 22/08/2018 on prevention and punishment of cybercrimes. These laws define electronic evidence, outline procedures for its collection, and establish penalties for cyber offenses. For instance, Article 38 of the cybercrime law stipulates that electronic evidence is admissible in court provided it meets the criteria of authenticity, integrity, and reliability. This provision aligns with international standards such as the Budapest Convention on Cybercrime, to which Rwanda

is a signatory. The legal framework also recognizes digital documents, electronic messages, and metadata as valid forms of evidence (Law No. 60/2018, 2018). Despite these legal advancements, gaps remain in the practical application of electronic evidence. Rwanda's legal provisions often lack detailed guidelines on preserving digital evidence and ensuring its chain of custody, leading to challenges in establishing its credibility in court.

Institutional challenges and technical gaps in implementing legal provisions

The effective enforcement of Rwanda's cybercrime and electronic evidence laws is hampered by institutional and technical deficiencies. Law enforcement agencies and the judiciary often lack specialized training and resources to handle digital evidence adequately. The National Public Prosecution Authority (NPPA) and the Rwanda Investigation Bureau (RIB) are the primary bodies responsible for investigating and prosecuting cybercrime cases, yet they face capacity limitations in digital forensics and cybersecurity expertise. One significant challenge is the absence of a dedicated cybercrime court, which results in generalist judges handling complex technical cases without sufficient background in electronic evidence. Additionally, there is a shortage of forensic experts and advanced technological tools needed for the proper acquisition and analysis of digital evidence.

Technical gaps also extend to the infrastructure for cross-border data access and cooperation with international partners. The lack of mutual legal assistance treaties (MLATs) with key jurisdictions often delays the collection of electronic evidence stored outside Rwanda, undermining the efficiency of cybercrime investigations (Kabano & Habarurema, 2023). A concrete example of this challenge is where Rwandan authorities faced significant delays in obtaining electronic evidence from a social media company headquartered in the United States. Due to the absence of a mutual legal assistance treaty (MLAT) between Rwanda and the U.S., the request for access to the suspect's online communications took several months, impeding the progress of the investigation and allowing the suspect more time to destroy potential evidence. This example highlights the urgent need for more bilateral agreements to streamline international cooperation in cybercrime investigations.

Rwandan court decisions on the use and admissibility of electronic evidence in cybercrime cases

Rwandan courts increasingly rely on electronic evidence when dealing with cybercrime and cyber-enabled offenses, particularly in cases involving mobile money fraud, unauthorized access to computer systems, and online financial

crimes. Because many cybercrime offenses are punishable by less than five years' imprisonment, they are usually tried before Primary Courts and Intermediate Courts, where most of Rwanda's digital-evidence jurisprudence has developed (Law No. 60/2018).

Across different courts, a consistent judicial approach can be observed: electronic evidence is admissible only when its authenticity, integrity, and origin can be reliably established. Rwandan judges place particular weight on whether the data was produced by a recognized and regulated custodian, such as a mobile network operator, a bank, or a mobile money provider, and whether the manner of collection and preservation is properly documented (URL13). This approach is illustrated in *Prosecution v. Dedan Muchoki Muriuki et al.* (Case No. RP/ECON 00002/2020/TGI/GSBO, Gasabo Intermediate Court, 30 June 2021). The case concerned a large-scale cyber-fraud scheme involving unauthorized access to computer systems and fraudulent mobile money transfers from Equity Bank. The prosecution relied on forensic images of mobile phones and computers, transaction logs, and telecommunications metadata to link the accused to the crimes. The court admitted this evidence only after the prosecution produced seizure records, forensic reports containing hash values, and sworn statements from investigators, demonstrating that the digital material had been preserved and extracted using scientifically reliable methods. The court made it clear that electronic evidence would not be admissible if its integrity could not be technically verified. A similar approach was applied by the Gasabo Primary Court in *Prosecution v. Muhimpundu Agnès* (Judgment of 5 December 2022). In this case, the accused was convicted of publishing defamatory content through electronic communication. The court relied on digital messages and online content only after establishing a clear link between the accused and the electronic account from which the information was disseminated. The decision shows that even in less complex cybercrime cases, courts require reliable attribution of electronic data to the person charged. More recently, the Gasabo Intermediate Court reaffirmed these principles in *Prosecution v. Cyiza Ezechiel & Ishimwe Josué* (Case No. RP/ECON 00045/2023/TGI/GSBO, 17 January 2024). The case involved the misappropriation of funds through mobile money transfers by an employee of a telecommunications company. The court relied on MTN transaction logs, expert reports, and internal system records to establish the electronic trail of the stolen money. These records were treated as highly reliable because they were generated and certified by the service provider and supported by expert testimony. Rwandan courts also distinguish between admissibility and evidentiary weight. Even when electronic records are formally admissible, judges examine whether they are corroborated

by other evidence, such as witness testimony, timing consistency, or CCTV footage. Where the defense raises reasonable doubts, for example by alleging SIM card fraud or third-party use of a device, courts may require additional supporting evidence or reduce the weight given to the digital data (Rwanda Investigation Bureau, 2023). Despite clear progress, challenges remain. In some cases, chain-of-custody documentation is incomplete, and forensic capacity varies between investigative units. Courts therefore sometimes admit electronic evidence only after requiring expert validation or additional corroboration. Nevertheless, the overall trend in Rwandan jurisprudence is clear: judges accept electronic evidence when it is technically verified, properly documented, and traceable to a lawful source, while excluding or discounting digital material that lacks procedural or forensic reliability.

Comparative evaluation of electronic evidence systems in Germany, Hungary, Estonia, and Rwanda

The regulation of electronic evidence in criminal proceedings is shaped by both international standards and domestic legal systems. Within Europe, a highly coordinated framework governs the collection, preservation, and admissibility of electronic evidence, primarily based on the Convention on Cybercrime (Budapest Convention) and its Additional Protocols (Council of Europe, 2001). EU Member States such as Germany, Hungary, and Estonia have incorporated these instruments into their national laws, creating systems that combine effective cybercrime enforcement with strong judicial safeguards and data protection standards. Rwanda is also a State Party to the Budapest Convention, following its accession through Presidential Order No. 020/01 of 26 January 2024, published in the Official Gazette of 21 March 2024. Rwanda is therefore legally bound by the Convention's obligations relating to the criminalization of cyber offenses, procedural powers for electronic evidence, and international cooperation. This places Rwanda within the same international normative framework as EU Member States. The difference between Rwanda and the EU countries examined in this study lies not in formal membership of the Convention, but in the extent to which its rules have been translated into detailed and operational domestic procedures. In the EU, the Budapest Convention is implemented through national criminal procedure laws and reinforced by EU instruments such as the European Investigation Order (Directive 2014/41/EU) and the evolving EU e-Evidence framework, which allow judicial authorities to request and obtain electronic data across borders in a fast and legally secure manner (European Parliament and Council, 2014). These mechanisms en-

sure that digital evidence can be preserved, produced, and exchanged while remaining subject to judicial oversight, proportionality, and data protection guarantees. Germany, Hungary, and Estonia apply these standards in different but complementary ways. Germany's Code of Criminal Procedure (StPO) requires judicial authorization for intrusive digital investigative measures and obliges courts to assess the legality, authenticity, and proportionality of electronic evidence (Noerr, 2023). Hungary implements the Budapest Convention through its Criminal Code (Act C of 2012) and Criminal Procedure Act (Act XC of 2017), which regulate the seizure, forensic examination, and international exchange of electronic data in cybercrime cases. Estonia, as a highly digitalized state, operates advanced e-forensics and electronic authentication systems within its Code of Criminal Procedure, including secure digital logs and electronic chain-of-custody mechanisms that ensure the integrity and traceability of electronic evidence from collection to trial. Rwanda, while formally aligned with these international standards, remains at an earlier stage of domestic implementation. Its principal legal instruments, the ICT Law (Law No. 24/2016) and the Cybercrime Law (Law No. 60/2018), recognize electronic evidence and criminalize cyber offenses (Republic of Rwanda, 2016; 2018). However, although Article 38 of the Cybercrime Law accepts electronic evidence in principle, Rwandan legislation does not yet provide detailed procedural rules on digital preservation, forensic verification, service provider cooperation, or cross-border data access comparable to those found in EU systems. As a result, Rwandan courts often rely on general evidentiary principles and judicial discretion when evaluating electronic evidence, rather than on a comprehensive statutory framework. This creates a situation in which Rwanda is normatively aligned with Europe through the Budapest Convention, but procedurally less developed at the national level. While EU Member States operate within mature systems that integrate forensic standards, judicial control, and cross-border cooperation into everyday practice, Rwanda is still building the institutional and technical structures required to give full effect to its international obligations. In general, the comparison shows that Germany's procedural precision, Hungary's legislative alignment with international instruments, and Estonia's digital-first forensic environment illustrate the advantages of clear legal rules, specialized institutions, and strong technological capacity. Rwanda has made important progress by acceding to the Budapest Convention, but its electronic evidence system would benefit from more detailed implementing legislation, stronger forensic infrastructure, and enhanced international cooperation mechanisms. These reforms would significantly improve the reliability,

admissibility, and credibility of electronic evidence in Rwanda's cybercrime prosecutions.

Lessons from the European Union for Rwanda's framework on electronic evidence

The comparative analysis of Germany, Hungary, Estonia, and Rwanda shows that effective use of electronic evidence depends not only on international commitments, but also on how those commitments are implemented in domestic law and practice. Although Rwanda has acceded to the Budapest Convention on Cybercrime, important differences remain between Rwanda's system and the more developed frameworks found in the European Union. This section draws on EU experience to identify practical lessons that can help Rwanda strengthen its legal, institutional, and technical framework for handling electronic evidence in cybercrime investigations and prosecutions.

Procedural clarity and legal harmonisation

EU Member States apply detailed procedural rules governing the collection, preservation, and admissibility of electronic evidence. Germany's Strafprozessordnung (StPO) and Hungary's Criminal Procedure Act (Act XC of 2017) require judicial authorization for digital searches and set clear standards for authenticity and legality, in line with the European Investigation Order (European Parliament and Council, 2014). Rwanda would benefit from adopting similarly explicit procedural provisions to ensure consistency and legal certainty in cybercrime cases.

Institutional cooperation and specialization

The EU's use of institutions such as Europol and Eurojust enables effective coordination in cross-border cybercrime investigations. Europol's SIRIUS Project provides a practical model for cooperation between law enforcement authorities and service providers when obtaining electronic evidence (Europol, 2024). Establishing specialized cybercrime units and strengthening interagency cooperation would significantly enhance Rwanda's investigative and prosecutorial capacity.

Judicial oversight and data protection

EU law, particularly the General Data Protection Regulation (GDPR), ensures that electronic evidence is collected and used with respect for privacy and fundamental rights (European Parliament and Council, 2016). Rwanda should strengthen judicial authorization and supervision of digital searches and data access to balance effective investigations with individual rights.

Digital forensic capacity building

EU Member States invest heavily in digital forensics, expert training, and secure electronic evidence systems, which increase the reliability and admissibility of electronic evidence (Juszczak & Sason, 2023). Rwanda would benefit from expanding forensic laboratories, training judges and prosecutors, and developing expert certification in digital evidence.

Summary of thought

This research shows that electronic evidence is central to the investigation and prosecution of cybercrime. However, its effective use depends on the strength of the legal rules, institutions, and technical systems that govern how digital data is collected, preserved, and presented in court. The comparison of Germany, Hungary, Estonia, and Rwanda highlights important differences in how these systems operate. In the European Union, electronic evidence is managed through well-developed and coordinated frameworks. EU countries benefit from harmonized laws, clear procedural rules, strong judicial oversight, and advanced digital forensic capacity. These national systems are supported by international and regional instruments such as the Budapest Convention on Cybercrime, the European Investigation Order, and the EU e-Evidence framework, which make it possible to obtain and use electronic data across borders while still protecting fundamental rights. Rwanda has made important progress through laws such as Law No. 60/2018 on Cybercrime and Law No. 24/2016 on ICT, and by acceding to the Budapest Convention. Nevertheless, Rwanda still faces challenges, including limited forensic capacity, unclear procedural rules for digital evidence, and insufficient institutional specialization. These weaknesses make it harder to ensure the consistent authenticity, preservation, and admissibility of electronic evidence, especially in cases involving foreign service providers or cross-border data. The EU experience offers practical guidance for addressing these gaps. Clearer procedural rules, specialized cybercrime units, stronger judicial oversight, better training, and investment in

digital forensic tools would significantly improve Rwanda's ability to handle electronic evidence. Adopting these best practices would not only strengthen Rwanda's response to cybercrime but also increase international confidence in its justice system. In conclusion, closing the gap between Rwanda and the EU in the governance of electronic evidence is essential for building a modern, effective, and rights-based criminal justice system capable of responding to the growing challenges of cybercrime.

References

Abdullah, M., Khan, A., Ali, S., & Rahman, F. (2025). Evolution of cybercrime - Key trends, cybersecurity threats, and mitigation strategies from historical data. *Analytics, 4*(3), Article 25. https://doi.org/10.3390/analytics4030025

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure, Policy and Development, 8*(10), Article 6007. https://doi.org/10.24294/jipd.v8i10.6007

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime. *World Journal of Advanced Research and Reviews, 21*(2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Antwi-Boasiako, A., & Venter, H. (2017). A model for digital evidence admissibility assessment. In Kechadi, B. T., Baggili, I., & Probst, W. C. (Eds.), *13th IFIP International Conference on Digital Forensics.* 23–38. Springer. https://doi.org/10.1007/978-3-319-67208-3_2

Brown, C. S. D. (2015). Investigating and prosecuting cybercrime. *International Journal of Cyber Criminology, 9*(1), 55–119. https://doi.org/10.5281/zenodo.22387

Buçaj, E. (2024). The need for cybercrime regulation. *Multidisciplinary Reviews, 8*(1), Article 2025024. https://doi.org/10.31893/multirev.2025024

Casino, F., Pina, C., López-Aguilar, P., & Batista, E. (2022). Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8*(1), 1-18. https://doi.org/10.1093/cybsec/tyac014

Cerezo, A. I., Lopez, J., & Patel, A. (2007). International cooperation to fight transnational cybercrime. In *Digital Forensics and Incident Analysis (WDFIA 2007)* 1–6. IEEE. https://doi.org/10.1109/WDFIA.2007.4299369

Ferreira, D. B., & Gromova, E. A. (2023). Electronic evidence in arbitration proceedings. *Digital Evidence and Electronic Signature Law Review, 20*, 30–39.

Hadjab, A. (2025). *Digital transformation and the evolving landscape of contemporary crime*. Université de M'Sila. https://www.researchgate.net/publication/394511675

Juszczak, A., & Sason, E. (2023). The use of electronic evidence in the EU. *Eucrim*. https://doi.org/10.30709/eucrim-2023-014

Kabano, J., & Habarurema, J. P. (2023). Procedural aspects of cybercrime investigations in Rwanda. *Makerere Law Journal, 52*(5), 240–266.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Columbia Law Review, 105*, 279–318.
Mifsud Bonnici, J. P., Tudorica, M., & Cannataci, J. A. (2018). The European legal framework on electronic evidence: Complex and in need of reform. In *Handling and exchanging electronic evidence across Europe* (pp. 189–234). Springer. https://doi.org/10.1007/978-3-319-74872-6_11
Narasimhan, P., & Kala, N. (2024). Ensuring the integrity of digital evidence. *International Journal of Scientific Research in Computer Science Engineering and Information Technology, 10*(6), 2438–2450. https://doi.org/10.32628/CSEIT2410612443
Szongoth, Z. V. R. (2024). Europol cooperation in Hungarian law enforcement. *Belügyi Szemle, 72*(9), 1669–1684. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i9.pp1669-1684
Thayer, J. B. (1890). The burden of proof. *Harvard Law Review, 4*(2), 45–70.
Wahl, T. (2023). E-evidence regulation and directive published. *Eucrim, 2*, 165–168.

Legal instruments

Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185).*
Directive 2014/41/EU of the European Parliament and of the Council on the European Investigation Order. *Official Journal of the European Union*, L130, 1–36.
Germany. (1949/2023). *Grundgesetz (GG) – Basic Law for the Federal Republic of Germany.* Federal Law Gazette.
Germany. (2017/2023). *Bundesdatenschutzgesetz (BDSG) – Federal Data Protection Act.* Federal Law Gazette.
Germany. (2023). *Strafgesetzbuch (StGB) – German Criminal Code.* Federal Law Gazette.
Germany. (2023). *Strafprozessordnung (StPO) – Code of Criminal Procedure.* Federal Law Gazette.
Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
Rwanda. (2016). *Law No. 24/2016 of 18 June 2016 governing information and communication technologies.* Official Gazette of the Republic of Rwanda, No. 26 of 27 June 2016.
Rwanda. (2018). *Law No. 60/2018 of 22 August 2018 on the prevention and punishment of cybercrimes.* Official Gazette of the Republic of Rwanda, Special Issue of 25 September 2018.

Court judgments

Federal Constitutional Court of Germany. (2008). *Online-Durchsuchung* (BVerfGE 115, 320).
Supreme Court of Rwanda. (2013, November 8). *Prosecution v. Nshimiyimana* (Case No. RPAA 0034/10/CS).

Gasabo Intermediate Court. (2021, June 30). *Prosecution v. Dedan Muchoki Muriuki et al.* (Case No. RP/ECON 00002/2020/TGI/GSBO).
Gasabo Primary Court. (2022, December 5). *Prosecution v. Muhimpundu Agnès* (Case No. RP 02289/2022/TB/GSBO).
Gasabo Intermediate Court. (2024, January 17). *Prosecution v. Cyiza Ezechiel & Ishimwe Josué* (Case No. RP/ECON 00045/2023/TGI/GSBO).

Online links in the article

URL1: Singla, P. (2025). *The impact of technology on criminal investigations and evidence*. *International Journal of Creative Research Thoughts, 13*(3), 1–10. https://www.ijcrt.org/papers/IJCRT25A3457.pdf
URL2: European Union Agency for Cybersecurity (ENISA). (2021). *ENISA threat landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
URL3: United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
URL4: ProvenData. (2021). *Cybersecurity best practices in 2025: How to ensure your data protection*. https://www.provendata.com/blog/cyber-security-best-practices/
URL5: Loux, M., & Loux, B. (2025). *How is digital evidence preserved in modern investigations?* https://www.amu.apus.edu/area-of-study/criminal-justice/resources/how-is-digital-evidence-preserved/
URL6: European Commission. (2021). *Proposal for a Council decision authorising Member States to ratify the Second Additional Protocol to the Convention on Cybercrime* (COM(2021) 719 final). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0719
URL7: Bachmaier, L. (2023). *Mutual admissibility of evidence and electronic evidence in the EU*. *Eucrim*. https://eucrim.eu/articles/mutual-admissibility-of-evidence-and-electronic-evidence-in-the-eu/
URL8: Eurojust. (2024). *The EU electronic evidence legislative package*. https://www.eurojust.europa.eu/publication/eu-electronic-evidence-legislative-package
URL9: Galli, F. (2018). *Law enforcement access to electronic data in cross-border criminal investigations*. European University Institute. https://cjc.eui.eu/wp-content/uploads/2023/07/JUD-IT-State-of-the-Art-Report-No.2-EUI-GALLI.pdf
URL10: Hungary. (2012). *Act C of 2012 on the Criminal Code*. https://thb.kormany.hu/download/a/46/11000/Btk_EN.pdf
URL11: Carrera, S., & Stefan, M. (2020). *Access to electronic data for criminal investigations purposes in the EU* (CEPS Paper No. 2020-01). https://cdn.ceps.eu/wp-content/uploads/2020/02/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf

URL12: Estonia. (2016). *Penal Code (Karistusseadustik) and Code of Criminal Procedure (Kriminaalmenetluse seadustik)*. https://www.riigiteataja.ee/en/eli/527012016001/consolide
URL13: Rwanda Investigation Bureau. (2023). *RIB – The 2017–2023 journey*. https://www.rib.gov.rw

Recommended citation

Nshimiyimana, F. R. (2026). Cross-border admissibility of electronic evidence in cybercrime investigations: Lessons from the European Union for Rwanda. *Belügyi Szemle, 74*(10), 2759–2787. https://doi.org/10.38146/bsz-ajia.2026.v74.i10.pp2759-2787

Declarations

Conflict of interest

The author declared no conflicts of interest.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Ethics statement

The author declares that the study was conducted in accordance with the applicable research ethics and publication ethics requirements.

Data availability

The research data supporting the findings presented in this study are available from the corresponding author upon reasonable request, subject to applicable data protection and other legal restrictions.

Open access

This article is published under the terms of the Creative Commons Attribution–NonCommercial–NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). The article may be freely shared and redistributed in any medium or format for non-commercial purposes, provided that it remains unchanged and appropriate credit is given to the original author(s) and the source of publication, together with a link to the licence. Distribution of modified or adapted versions and commercial use are not permitted under this licence.

Corresponding author

The corresponding author of this article is Nshimiyimana Francois Regis, who can be contacted at *regisnshimiye82@gmail.com*.