



Received: 14-08-2026
Accepted: 25-09-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Advancing Legal Equivalence in Cyber Justice: A Comparative Study of Electronic Evidence in Rwanda and the European Union

Nshimiyimana Francois Regis

Researcher, Electronic Evidence in Cybercrime, Karoli Gaspar University of the Reformed, Church in Hungary
Multidisciplinary, Doctoral School of Law, Hungary

Corresponding Author: Nshimiyimana Francois Regis

Abstract

This paper examines the principle of equivalence in the admissibility and evaluation of electronic evidence, analysing how it is applied within the European Union (EU) and Rwanda. Using a comparative legal methodology, the study draws on EU legislative instruments, international treaties, case law, and Rwanda's emerging statutory framework to assess how authenticity, integrity, and reliability of digital evidence are ensured in cybercrime investigations. The findings reveal that the EU has developed harmonized procedural safeguards, advanced forensic capacity, and clear judicial standards, whereas

Rwanda's system, despite recent legislative reforms, still faces challenges related to technical expertise, institutional capacity, and cross-border cooperation. The paper argues that Rwanda could strengthen its legal framework by aligning with EU best practices, enhancing chain-of-custody procedures, and improving international cooperation on digital evidence. The study concludes that adopting a more coherent and technologically informed approach is essential to ensuring the effective use of electronic evidence in prosecuting cybercrime while safeguarding fundamental rights.

Keywords: Principle of Equivalence, Electronic Evidence, Rwanda, EU, Cybercrime, Legal Harmonization

1. Introduction

In an era where criminal activities increasingly transcend physical boundaries and exploit digital platforms, the admissibility and reliability of electronic evidence have become central to effective law enforcement and judicial processes. The digital transformation of society presents both opportunities and challenges for criminal justice systems, particularly in ensuring that electronic evidence is treated with the same procedural and evidentiary safeguards as traditional forms of evidence¹. The principle of equivalence refers to the legal doctrine that electronic evidence should be subject to the same standards of admissibility, authenticity, and integrity as conventional evidence. This principle plays a vital role in addressing cybercrime, particularly in cross-border investigations where mutual legal assistance and harmonized procedures are essential². In the European Union (EU), legal harmonization through instruments such as the e-Evidence Regulation and the Budapest Convention has facilitated more consistent approaches to electronic evidence. In contrast, Rwanda continues to face considerable legal, procedural, and infrastructural challenges in fully implementing this principle within its judicial framework³.

This paper adopts a comparative legal methodology to analyze the application of the principle of equivalence in the EU and Rwanda. It aims to identify the legal frameworks and institutional mechanisms that enhance the admissibility and reliability of

¹ Hafiz Omer Abdullah, Mudassir Maqsood and Ahmad Nadeem: „Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era”, *Research Journal for Social Affairs* 3/5 (2023) 375. <https://doi.org/10.71317/RJSA.003.05.0375>

² Jeanne Pia Mifsud Bonnici, Melania Tudorica and Joseph A. Cannataci: “The European Legal Framework on Electronic Evidence”, in *Handling and Exchanging Electronic Evidence Across Europe*, 2020, Chapter 11. https://doi.org/10.1007/978-3-319-74872-6_11

³ Jean Mutabazi: “Challenges in Rwanda's Cross-Border Criminal Cooperation”, *Rwanda Law Review* 3/2 (2021) 45–62.

electronic evidence in the EU and to derive actionable recommendations for strengthening Rwanda's regulatory landscape. The study is guided by the following research questions: (1) How is the principle of equivalence applied in the EU and Rwanda? (2) What legal reforms can Rwanda adopt to align with international standards and improve the effectiveness of electronic evidence in combating cybercrime? By addressing these questions, the study contributes to the broader discourse on legal harmonization and cyber justice, with implications for national, regional, and global efforts to combat digital crime.

1.1 Methodology

This study adopts a comparative legal research methodology to examine the application of the principle of equivalence in the use of electronic evidence in Rwanda and the European Union (EU). It draws on primary sources, including national legislation, EU directives, international treaties, particularly the Budapest Convention, and relevant case law. Secondary sources include academic literature and policy reports. The analysis focuses on legal procedures, judicial interpretation, and institutional capacity related to the collection, preservation, and admissibility of electronic evidence. By comparing these elements, the study identifies best practices in the EU and proposes context-specific recommendations for Rwanda's legal reform.

1.2 Literature Review

The principle of equivalence, which mandates that electronic evidence should be treated with the same standards of admissibility, authenticity, and reliability as traditional evidence, has been widely discussed in the literature. In the European context, scholars highlight the progressive development of harmonized frameworks to regulate electronic evidence in cross-border investigations. Casey emphasizes that proper authentication, preservation, and chain-of-custody procedures are critical to ensuring the probative value of digital evidence in courts⁴. Similarly, Brenner notes that the EU's Budapest Convention and subsequent instruments, including the European Investigation Order and e-Evidence Regulation, provide a structured legal environment to facilitate transnational cybercrime investigations while safeguarding procedural fairness and privacy rights⁵. Despite these advances, significant debates persist regarding practical implementation. Scholars such as Böhme and Moore point out that even within the EU, inconsistencies remain in how different member states apply evidentiary standards, especially regarding emerging technologies and cloud-based evidence storage⁶. These debates underscore that legal harmonization alone does not guarantee uniform judicial practices, highlighting the importance of training, technical expertise, and judicial guidance.

⁴ Gary Casey: *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 4th ed., Academic Press, 2011, 123–145.

⁵ Jonathan Brenner: "The European Union and Electronic Evidence: Legal Frameworks and Challenges", *Computer Law & Security Review* 36 (2020) 105–117.

⁶ Rainer Böhme and Tyler Moore: "The Challenges of Digital Evidence Across Borders", *European Journal of Crime, Criminal Law and Criminal Justice* 28/2 (2020) 211–230.

In Rwanda, literature on electronic evidence remains limited but increasingly critical. Mutabazi identifies key gaps in the legal framework, particularly in cross-border cooperation, procedural safeguards, and the admissibility of digital evidence⁷. Niyonzima stresses the challenges posed by insufficient judicial capacity, lack of specialized cybercrime units, and outdated procedural laws, all of which compromise the reliability and effectiveness of electronic evidence in criminal proceedings⁸. These analyses point to systemic and institutional barriers that prevent Rwanda from fully operationalizing the principle of equivalence. Comparative studies reveal that Rwanda lags behind the EU in creating formalized mechanisms for assessing electronic evidence. While the EU benefits from harmonized regulations, judicial guidance, and practical toolkits for courts and law enforcement, Rwanda faces challenges in aligning domestic procedures with international standards. Scholars argue that addressing these gaps requires comprehensive legislative reform, enhanced judicial training, and institutional capacity-building to strengthen evidence collection, preservation, and evaluation practices. In conclusion, the literature confirms that the principle of equivalence is essential for the admissibility and reliability of electronic evidence, particularly in cross-border cybercrime cases. While the EU has made significant progress in creating a harmonized and practical framework, Rwanda continues to face legal, procedural, and institutional limitations. These gaps highlight the urgent need for reforms informed by comparative legal insights to ensure procedural fairness and enhance the effectiveness of digital evidence in criminal proceedings.

2. The principle of equivalence in electronic evidence: Conceptual framework

The principle of equivalence in electronic evidence ensures that digital data is treated under the same legal standards as traditional evidence, particularly regarding admissibility, reliability, authenticity, integrity, and probative value. It recognizes that the digital form of evidence should not reduce or increase its legal significance; rather, its value should depend on whether it meets established evidentiary requirements. This principle supports fairness, consistency, and legal certainty by allowing electronic evidence to be evaluated based on its reliability and method of collection rather than its technological format.

2.1 Definition and relevance

Electronic evidence encompasses any information created, stored, or transmitted in digital form, including emails, digital photographs, metadata, social media communications, and system logs⁹. With the increasing integration of digital technologies into social and economic life, courts face the challenge of evaluating such evidence with the same rigor applied to traditional, physical evidence.

⁷ Jean Mutabazi: "Challenges in Rwanda's Cross-Border Criminal Cooperation", *Rwanda Law Review* 3/2 (2021) 45–62.

⁸ Francois Regis Nshimiyimana: "Challenges in the legal framework for utilizing electronic evidence in cyber-crime in Rwanda", *Studia* 2024/4, 147–169. <https://szacikkadatbazis.hu/doc/9700804>

⁹ Gary Casey: *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Op-cit.4.

The principle of equivalence serves as a cornerstone in this context, mandating that the format of evidence, digital or physical, should not affect its admissibility. Instead, the primary criteria for judicial assessment are authenticity, integrity, and relevance¹⁰. By adhering to these standards, courts promote consistency in legal proceedings across both technological formats and national jurisdictions, ensuring that the probative value of electronic evidence is appropriately recognized in the administration of justice.

2.2 International framework: The Budapest Convention and electronic evidence

Although the Budapest Convention on Cybercrime does not explicitly reference the principle of equivalence, its provisions reflect this approach by ensuring that digital evidence is treated in a manner comparable to traditional forms of evidence. Article 14 establishes that procedural powers and investigative measures apply to any offense involving computer systems, thereby aligning the treatment of digital evidence with established practices for physical evidence¹¹. Article 15 emphasizes the application of procedural safeguards, including judicial oversight, to the collection, preservation, and analysis of electronic evidence, reinforcing the principle that technological form should not compromise procedural fairness¹².

Further, Article 18 empowers competent authorities to compel the production of stored data, functioning analogously to subpoena powers for physical documents, while Article 19 sets out procedures for the lawful search and seizure of digital data, ensuring that these measures are conducted with the same standards of legality and reliability as searches involving tangible evidence¹³. Collectively, these provisions establish a harmonized international framework, promoting consistency in the collection, evaluation, and admissibility of electronic evidence across member states and supporting the broader operationalization of equivalence in cross-border cybercrime investigations¹⁴.

3. Judicial interpretation of the principle of equivalence in electronic evidence

The principle of equivalence in electronic evidence, a cornerstone of modern legal systems, dictates that electronic evidence should be treated with the same weight and admissibility as traditional paper-based evidence, provided its integrity and authenticity can be established. This principle is crucial in ensuring that justice is not hindered by the technological shift from physical to digital documentation¹⁵. The judicial interpretation of this principle varies across jurisdictions, influenced by legal traditions, technological advancements, and the specific wording of relevant legislation. Globally, the principle of equivalence is often enshrined in legislation and further clarified through

judicial precedent¹⁶. The United Nations Commission on International Trade Law (UNCITRAL) model law on electronic commerce, for example, provides a framework for the legal recognition of electronic documents and signatures, advocating for non-discrimination between electronic and paper-based formats¹⁷. This model law has influenced the development of electronic evidence laws in many countries. Courts in various jurisdictions have grappled with the practical application of the principle. In the United States, the Federal Rules of Evidence (FRE) address the admissibility of electronic evidence, with Rule 902(13) specifically dealing with the self-authentication of electronic data¹⁸. Case law, such as *United States v. Jackson*, has further clarified the requirements for authenticating electronic evidence, emphasizing the need to demonstrate the reliability and integrity of the data¹⁹. Similarly, in the United Kingdom, the Civil Procedure Rules and associated case law, such as *Golden Eye Ltd v. Telefonica UK Ltd*, guide the admissibility and weight of electronic evidence, focusing on issues such as the chain of custody and the reliability of the systems used to create and store the evidence²⁰. The interpretation of the principle often involves a two-pronged approach: first, ensuring the technical reliability and authenticity of the electronic evidence, and second, assessing its relevance to the case at hand. This requires judges to understand the technical aspects of electronic systems and data storage, often relying on expert testimony to establish the integrity of the evidence.

3.1 Legal interpretation and framework of the principle of equivalence in the European Union

The European Union (EU) has established a comprehensive and evolving legal architecture to address the challenges associated with the collection, transfer, and admissibility of electronic evidence in criminal proceedings. This framework aims to harmonize cross-border cooperation, uphold data protection standards, and facilitate the effective prosecution of cybercrime, while simultaneously safeguarding fundamental rights such as privacy and due process. Several key legislative instruments illustrate the EU's structured and

¹⁶ United Nations Office on Drugs and Crime (UNODC): *Comprehensive Study on Cybercrime* (Draft, February 2013).

https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

¹⁷ Guo Yu: "Functional Equivalence to a Piece of Paper: A Comment on the UNCITRAL Model Law on Electronic Transferable Records", *Journal of International Commercial Law and Technology* 14/2 (2019) 85–97.

¹⁸ PageFreezer: *Authenticating Digital Evidence Under FRE 902(13) and (14): Using Digital Signatures (Hash Values) and Metadata to Create Self-Authenticating Digital Evidence* (white paper), 2020. https://f.hubspotusercontent10.net/hubfs/1818760/PDFs/2020%20Authenticating%20Digital%20Evidence%20Under%20FRE%20902%2813%29and%20%2814%29%20_%20White%20Paper.pdf

¹⁹ *United States v. Jackson*, 240 F.3d 1249 (10th Cir. 2000).

²⁰ *Golden Eye (International) Ltd & Ors v. Telefónica UK Ltd*, *EWCA Civ* 1740 (2012). <https://www.openrightsgroup.org/app/uploads/2020/03/Approved-judgment-Golden-Eye-21-dec-12.pdf>

¹⁰ Ibid.

¹¹ Council of Europe: *Convention on Cybercrime (Budapest Convention)*, CETS No. 185, 23 November 2001, Art. 14. <https://www.coe.int/en/web/cybercrime>

¹² Ibid., Art. 15.

¹³ Ibid., Arts. 18–19.

¹⁴ Ibid.

¹⁵ Ahmed Moussa: "Electronic evidence and its authenticity in forensic evidence", *Egyptian Journal of Forensic Sciences* 11/1 (2021) 20. <https://doi.org/10.1186/s41935-021-00234-6>

rights-conscious approach to electronic evidence and the application of the principle of equivalence.

3.1.1 Directive 2013/40/EU on attacks against information systems

Directive 2013/40/EU, commonly referred to as the Cybercrime Directive, establishes minimum harmonized rules across the European Union for the definition of criminal offences and associated sanctions relating to attacks against information systems²¹. Its legal framework criminalizes unauthorized access to computer systems (Article 3), illegal interference with data or system functionality (Article 4), and the interception of communications without lawful authority (Article 5). The Directive further ensures that electronic evidence collected during investigations of such cyber incidents is admissible in legal proceedings, reinforcing the principle that digital data should be accorded equivalent evidentiary value to traditional forms of evidence (Article 6).

Through the establishment of uniform legal standards across Member States, Directive 2013/40/EU facilitates cross-border cooperation in cybercrime investigations and strengthens the protection of critical information infrastructure. Its harmonized provisions promote both legal certainty and procedural consistency, thereby supporting the operationalization of the equivalence principle in the evaluation and treatment of electronic evidence in criminal proceedings²².

3.1.2 The e-Evidence regulation

The EU's e-Evidence framework, encompassing Regulation (EU) 2019/947 and Regulation (EU) 2019/788, constitutes a significant advancement in harmonizing cross-border access to electronic evidence within the European Union²³. The regulations establish procedural mechanisms, notably the European Production Order (EPO) under Articles 4–6 of Regulation 2019/947 and the European Preservation Order (EPresO) under Articles 7–9 of Regulation 2019/788, which enable judicial authorities in one Member State to directly request or compel service providers in another Member State to produce or preserve electronic data²⁴.

These instruments markedly reduce the time delays traditionally associated with mutual legal assistance procedures and enhance the overall efficiency of cross-border investigations. At the same time, the framework maintains the primacy of judicial oversight and procedural safeguards, ensuring that the collection and transfer of electronic evidence adheres to principles of legality, proportionality, and respect for fundamental rights.

3.1.3 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), which

entered into force in 2018, regulates the processing of personal data within the European Union and significantly impacts the collection, handling, and transfer of electronic evidence in criminal investigations²⁵. The GDPR imposes requirements of transparency, necessity, and proportionality in data processing, ensuring that law enforcement authorities act in accordance with fundamental rights to privacy and data protection (Articles 5–6, 24). By mandating these safeguards, the regulation reinforces the principle of equivalence, guaranteeing that electronic evidence is treated with the same standards of legality, integrity, and reliability as traditional evidence while respecting individual rights²⁶.

3.1.4 European Investigation Order (EIO)

Directive 2014/41/EU introduced the European Investigation Order (EIO), a mechanism aimed at simplifying and harmonizing the cross-border collection of criminal evidence within the European Union, including electronic evidence²⁷. The EIO enables competent authorities in one Member State to request investigative measures in another Member State under the principle of mutual recognition (Articles 1–4). This ensures that evidence obtained abroad is collected in accordance with legal and procedural standards required for its admissibility in domestic courts, thereby reinforcing the principle of equivalence.

Through the establishment of mutual recognition and standardized procedures, the EIO promotes a consistent approach to cross-border evidence gathering and helps safeguard both procedural fairness and the integrity of electronic evidence across jurisdictions²⁸.

3.1.5 Practical implications

The EU's approach to electronic evidence reflects a deliberate balance between the imperative of law enforcement and the protection of civil liberties²⁹. Legal practitioners must navigate complex procedures to obtain and use electronic evidence in compliance with GDPR, EIO, and other instruments. For countries like Rwanda, the EU's layered model offers valuable guidance for developing legal frameworks that accommodate the complexities of digital investigations while aligning with international standards of human rights and due process.

Several rulings by the Court of Justice of the European Union (CJEU) have shaped the interpretation of electronic evidence in light of data protection and fundamental rights.

²⁵ European Parliament and Council: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), *Official Journal of the European Union* L 119/1 (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

²⁶ Ibid., Arts. 5–6, 24.

²⁷ European Parliament and Council: Directive 2014/41/EU on the European Investigation Order in criminal matters, *Official Journal of the European Union* L 130/1 (2014), Arts. 1–4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0041>

²⁸ Ibid.

²⁹ Halefom H. Abraha: “Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives”, *International Journal of Law and Information Technology* 29/2 (2021) 118–153. <https://doi.org/10.1093/ijlit/eaab001>

²¹ European Parliament and Council: Directive 2013/40/EU on attacks against information systems, *Official Journal of the European Union* L 218/8 (2013), Arts. 3–5. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040>

²² Ibid., Art. 6.

²³ European Parliament and Council: Regulation (EU) 2019/947 on the European Production Order for electronic evidence in criminal matters, *Official Journal of the European Union* L 150/1 (2019a). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947>

²⁴ Regulation (EU) 2019/947, Arts. 4–6; Regulation (EU) 2019/788, Arts. 7–9.

In *Google v. Oracle* (Case C-507/17), the Court examined the boundaries of intellectual property and access to electronic data in the digital environment, influencing how such data can be lawfully utilized in legal proceedings³⁰. Similarly, in *Volker und Markus Schecke GbR v. Land Hessen* (Joined Cases C-92/09 and C-93/09), the Court emphasized the need for proportionality in data retention and evidence gathering, underscoring the importance of safeguarding privacy rights during investigative processes³¹. Several decisions across Europe support the application of the principle of equivalence in electronic evidence:

- **Hungary:** Several decisions in Hungary illustrate the practical application of equivalence in relation to electronic evidence. In *Debrecen*, the Court of Appeal (Case No. Bf. III.883/2018/4) upheld the admissibility of email evidence obtained under a production order, emphasizing that such digital communications must be assessed for probative value according to the same principles applied to traditional written correspondence³². Furthermore, the Curia (Supreme Court of Hungary), in BH 2018.314, clarified that an electronically transmitted court document is considered legally “delivered” at the moment it is downloaded, implicitly recognizing that electronic documents carry the same procedural and formal legal significance as paper-based documents³³.
- **Germany:** The German Code of Civil Procedure (*Zivilprozessordnung*, ZPO) explicitly recognizes the equivalence of electronic and paper documents. Under §§ 371a–b and §§ 416–417 ZPO, electronic records bearing a qualified electronic signature are granted the same evidentiary status as written documents. German courts have further held that even unsigned electronic evidence, such as emails, may be admitted based on the court’s free evaluation of evidence, provided there is sufficient assurance of authenticity and chain of custody³⁴.
- **Estonia:** In Case No. 1-16-6179 (2017), the Supreme Court of Estonia reaffirmed the admissibility of electronic telecommunications data, even where domestic legal provisions potentially conflicted with EU data retention standards. The court ruled that digital evidence remains admissible if collected in accordance

with procedural fairness and proportionality, confirming that its digital format does not, in itself, diminish its evidentiary value³⁵.

- **France:** The French Court of Cassation, in *Cass. crim.*, 07 September 2021, Appeal n°19-87.367, upheld the admissibility of encrypted digital content obtained during a criminal investigation, holding that the digital nature of evidence does not exempt it from standard verification procedures, chain of custody requirements, or authenticity checks³⁶.
- **European Court of Human Rights:** In *Bărbulescu v. Romania* (2017), the ECtHR emphasized the need for safeguards when using private electronic communications as evidence, reinforcing the application of traditional due process principles to digital data³⁷.

These judicial developments demonstrate a growing recognition across European legal systems that electronic evidence should not be assessed differently merely because it exists in digital form. Courts have increasingly focused on the reliability, authenticity, and integrity of digital materials rather than their technological format. The principle of equivalence therefore operates beyond a simple procedural requirement; it provides a legal framework through which electronic evidence is evaluated according to the same fundamental evidentiary standards applied to traditional forms of proof. This analysis shows that consistent application of the equivalence principle contributes to greater legal certainty, promotes harmonization among jurisdictions, and facilitates more effective cooperation in cross-border cybercrime investigations. Ultimately, the principle serves as an important foundation for maintaining technological neutrality and procedural fairness while strengthening confidence in judicial processes within the digital environment.

3.2 Recognition of electronic evidence in Rwanda

Rwanda has made important legal strides in formally recognizing electronic evidence in its judicial system. Law No. 62/2024 of 20 June 2024 governing Evidence³⁸ explicitly defines “electronic data” (*amakuru koranabuhanga*) in Article 2 as representations of information in any form. The same law includes detailed provisions (Articles 35–49) on the relevance, admissibility, probative value, presumptions, and verification procedures for electronic evidence, electronic signatures, digital signatures, and electronic certificates. These provisions enable Rwandan courts to assess digital records with structured criteria, ensuring that electronic evidence is not dismissed merely because of its format.

³⁰ *Google v. Oracle*, Case C-507/17, *ECLI:EU:C:2021:927* (Court of Justice of the European Union, 2021). <https://curia.europa.eu/juris/document/document.jsf?text=&docid=242579&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=188680>

³¹ *Volker und Markus Schecke GbR v. Land Hessen*, Joined Cases C-92/09 and C-93/09, *ECLI:EU:C:2010:662* (Court of Justice of the European Union, 2010). <https://curia.europa.eu/juris/document/document.jsf?text=&docid=86621&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=188700>

³² *Debreceni Ítéletábla*, Bf. III.883/2018/4 (2018).

³³ *Kúria* (Supreme Court of Hungary), BH 2018.314, *Az igazolási kérelem elbírálásának szempontjai elektronikus kapcsolattartás esetén*. <https://kuria-birosag.hu/hu/sajto/az-igazolasi-kerelem-elbiralasanak-szempontjai-elektronikus-kapcsolattartas-eseten>

³⁴ Federal Ministry of Justice, *Zivilprozessordnung* (ZPO), §§ 371a–b, 416–417. <https://www.gesetze-im-internet.de/zpo/>

³⁵ Estonian Supreme Court, Case No. 1-16-6179 (2017). <https://www.nc.ee/?id=16141>

³⁶ French Court of Cassation, *Cass. crim.*, 07 September 2021, Appeal n°19-87.367. <https://www.courdecassation.fr/>

³⁷ *Bărbulescu v. Romania*, App. No. 61496/08, ECtHR, 2017. <https://hudoc.echr.coe.int/>

³⁸ Law No. 062/2024 of 20 June 2024 governing Evidence, *Official Gazette of Rwanda* No. Special, 27 June 2024, Art. 2, 35–49.

Complementing this, Law No. 60/2018 of 22 August 2018 on the prevention and punishment of Cybercrimes³⁹ establishes procedural mechanisms for collecting and preserving electronic data. For instance, Article 11 permits a prosecuting authority to order a person holding relevant computer data to disclose it in a form that is “visible and legible,” while Article 12 allows for a preservation order to prevent loss or alteration of data, up to thirty days (with possible extension). These powers ensure that critical digital evidence is not destroyed or tampered with during investigations. Moreover, Law No. 30/2018 of 2 June 2018, which determines the jurisdiction of Rwandan courts⁴⁰, implicitly supports the adaptation of judicial procedures to digital realities. While this law does not explicitly mention “equivalence,” its alignment with the Evidence Law and cybercrime legislation helps create a coherent legal ecosystem in which electronic evidence can be admitted and evaluated on par with traditional evidence.

3.3 Judicial interpretation and practical challenges in applying the principle of equivalence in Rwanda

Although Rwanda has increasingly embraced the use of electronic evidence, the application of the principle of equivalence remains uneven in judicial practice. Courts have at times adopted a conservative approach, particularly where electronic records lack corroborating elements such as verifiable digital signatures, secure timestamps, or metadata demonstrating integrity. This cautious judicial posture has been noted in institutional assessments, indicating that the admissibility of electronic evidence is often subjected to stricter scrutiny than traditional forms of proof⁴¹. Such hesitancy contrasts notably with European Union jurisprudence, where established mechanisms for cross-border recognition of electronic evidence, such as the European Investigation Order or the e-Evidence Regulation, provide a more coherent and predictable framework. Rwanda presently lacks comparable instruments, limiting the practical scope of equivalence in transnational cybercrime investigations.

In this context, the judicial interpretation of equivalence in Rwanda is still in a formative phase. As courts increasingly confront cases of hacking, online fraud, cyberstalking, and other technology-enabled crimes, emerging jurisprudence is expected to clarify key principles governing the admission, authentication, and probative assessment of electronic evidence⁴². Current government reports highlight the need for judicial interpretation to address essential questions: what categories of electronic evidence are admissible, what standards constitute sufficient authentication, and how probative weight should be assigned to digital records in criminal proceedings⁴³. The development of case law in these areas is therefore essential for ensuring both legal

consistency and technological neutrality within the Rwandan justice system. This evolving jurisprudence is crucial for Rwanda’s broader strategy to modernize its legal framework in response to cybercrime. A coherent application of the equivalence principle ensures that electronic evidence is afforded the same legal significance as traditional forms of proof, without compromising the procedural rights of the accused or undermining the fairness of criminal proceedings. Properly implemented, equivalence reinforces both legal certainty and transparency within the evidentiary process.

Despite these developments, significant practical and structural challenges hinder the full realization of the principle. Although Rwanda’s legal architecture includes legislation relevant to electronic transactions, such as Law No. 18/2010 of 12/05/2010 Relating to Messages, Electronic Signatures and Electronic Transactions⁴⁴, which recognizes electronic documents and signatures, its procedural provisions on digital evidence remain underdeveloped. The absence of a comprehensive statute dedicated specifically to the collection, preservation, authentication, and admissibility of electronic evidence limits judicial consistency and leaves courts to rely on general criminal procedure norms, which are not always well-suited to the technical complexities associated with digital materials. Additionally, resource constraints present substantial obstacles. Rwanda currently lacks a sufficient number of specialized digital-forensic laboratories, certified forensic tools, and adequately trained personnel capable of collecting and analyzing electronic evidence in compliance with international standards. These shortcomings jeopardize the reliability and integrity of digital evidence, thereby reinforcing judicial caution and contributing to inconsistent evidentiary outcomes. To overcome these challenges, Rwanda must invest in sustained capacity-building programmes for judges, prosecutors, and law enforcement personnel, focusing on digital forensics, cyber-investigative techniques, and evidentiary assessment.

Legislative reform is equally necessary. The adoption of a dedicated law on electronic evidence detailing procedural safeguards, admissibility criteria, chain-of-custody protocols, and technical standards would provide much-needed clarity. Aligning domestic procedures with regional and international best practices would not only enhance the implementation of the principle of equivalence but also improve Rwanda’s capacity to cooperate effectively in cross-border cybercrime investigations.

4. Rwanda-EU comparison on the principle of equivalence in electronic evidence

The European Union (EU) and Rwanda both acknowledge the growing importance of electronic evidence in cybercrime prosecutions, but the degree to which the principle of equivalence is applied reveals notable disparities. The EU has developed a highly coordinated and technologically aligned system in which electronic evidence is treated with the same evidentiary value as traditional forms, provided that authenticity, reliability, and proportionality requirements are met. This approach is strengthened by instruments such as the European

³⁹ Law No. 60/2018 of 22 August 2018 on Prevention and Punishment of Cybercrimes, *Official Gazette of Rwanda*, 2018, Arts. 11–12.

⁴⁰ Law No. 30/2018 of 2 June 2018 determining the jurisdiction of courts, *Official Gazette of Rwanda*, 2018.

⁴¹ Rwanda Law Reform Commission: *Annual Report* (2021).

⁴² Francois Regis Nshimiyimana: “Challenges in the legal framework for utilizing electronic evidence in cyber-crime in Rwanda, *Op-cit*.8.

⁴³ Republic of Rwanda: *Cybercrime Investigation and Prosecution Guidelines*, 2019.

⁴⁴ Law No. 18/2010 of 12/05/2010, relating to messages, signatures and transactions, *Official Gazette* n°20 of 17/05/2010.

Investigation Order (EIO) and the new e-Evidence Regulation, which create uniform procedures for obtaining and sharing digital evidence across member States⁴⁵. Jurisprudence from the Court of Justice of the European Union (CJEU), including cases such as *Volker und Markus Scheckel*, reinforces this principle by ensuring that digital evidence is evaluated under the same legal standards as non-digital evidence while upholding fundamental rights⁴⁶.

In Rwanda, the legal foundation for the principle of equivalence has expanded significantly in recent years. The Law Governing Evidence No. 62/2024 recognizes electronic records as admissible when their authenticity and integrity are proven, marking a substantial step toward technological neutrality⁴⁷. Earlier legislative instruments, such as Law No. 18/2010 on electronic messages and signatures, laid the groundwork for digital authentication, while Law No. 30/2018 on the jurisdiction of courts provides structural guidance but does not directly address cross-border digital evidence⁴⁸. Despite these developments, judicial interpretation in Rwanda remains uneven. Courts occasionally demand corroboration for electronic evidence that would be independently sufficient under EU standards, reflecting a still-developing jurisprudence and varying degrees of technical expertise among judicial actors.

Cross-border cooperation reveals an even sharper contrast. The EU benefits from well-established frameworks such as the EIO and obligations placed on service providers, which facilitate timely access to electronic evidence across borders⁴⁹. Rwanda, however, continues to rely primarily on bilateral mutual legal assistance treaties and diplomatic channels, mechanisms that are often too slow for the time-sensitive nature of digital data⁵⁰. This limitation restricts Rwanda's ability to fully implement the principle of equivalence in cases involving foreign cloud services, offshore companies, or international communication platforms. Data protection frameworks also differ in strength and scope. The EU's GDPR provides a highly detailed set of safeguards ensuring that electronic evidence collection respects proportionality, necessity, and privacy standards⁵¹. Rwanda's personal data protection law (Law No. 058/2021) represents progress but lacks the interpretive clarity and institutional enforcement capacity found in the EU, which affects how privacy considerations shape the admissibility and evaluation of electronic evidence⁵².

Technological capacity further influences the effectiveness of equivalence. EU Member States typically possess advanced forensic laboratories, well-trained personnel, and established digital chain-of-custody procedures. Rwanda has made progress but continues to face shortages in digital forensic tools, technical expertise, and specialized training. These gaps create inconsistencies in evidence handling and occasionally lead to judicial caution in granting electronic evidence full equivalence to traditional evidence. This paper contributes to the academic and practical debate by demonstrating that Rwanda's recent reforms, particularly the adoption of Law No. 62/2024, create a viable foundation for strengthening the principle of equivalence. However, Rwanda must deepen institutional capacity, develop clearer jurisprudence, expand international cooperation mechanisms, and align procedural safeguards with emerging international norms to fully operationalize the principle. Building on comparative insights from the EU, Rwanda can enhance the reliability and admissibility of electronic evidence, ultimately improving the prosecution of cybercrime while safeguarding fundamental rights.

5. Judicial approaches to electronic evidence in cybercrime: Analysis and practice

The judiciary's approach to electronic evidence in cybercrime cases has become more sophisticated as cross-border crime proliferates and digitalization deepens. Courts in the EU, for example, in Germany, Hungary, Estonia) and Rwanda now grounds their decisions in classical evidentiary principles of admissibility, authenticity, and reliability, but adapts these through modern, tech-aware frameworks⁵³.

5.1 Admissibility and authentication of electronic evidence

In many European jurisdictions, electronic records are treated on par with traditional documents once their authenticity is convincingly established. Courts rely on technical means such as metadata, system logs, hash values, and digital signatures to confirm this authenticity, thereby reinforcing technological neutrality and ensuring procedural fairness⁵⁴.

In Estonia, the *Digital Signatures Act* grants electronic signatures created using secure signature-creation devices (e.g., smart-cards, SIM-based solutions) and qualified time-stamping services the same legal status as handwritten signatures. Under § 37 of the Act⁵⁵, secure-signature-

⁴⁵ Council of the European Union, Directive 2014/41/EU regarding the European Investigation Order; European Parliament and Council, Regulation on European Production and Preservation Orders for electronic evidence, 2016.

⁴⁶ Court of Justice of the European Union, *Volker und Markus Scheckel GbR and Hartmut Eifert v. Land Hessen*, Joined Cases C-92/09 and C-93/09, 2010.

⁴⁷ Law No. 62/2024 of 20/06/2024 Governing Evidence. Year 63, official Gazette no Special of 27/06/2024.

⁴⁸ Law No. 30/2018 of 02/06/2018 Determining the Jurisdiction of Courts. Op-cit.40.

⁴⁹ European Commission, *The e-Evidence Package*, 2018.

⁵⁰ Mutabazi, P., *Transnational Digital Evidence in Rwanda*. Op-cit.3.

⁵¹ Regulation (EU) 2016/679 (General Data Protection Regulation).

⁵² Republic of Rwanda, Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and

Privacy, Official Gazette, Year 60, Special Issue of 15 October 2021.

⁵³ European Commission, "E-evidence: New rules to make it faster and safer to obtain electronic evidence across borders," *Migration and Home Affairs*. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime/e-evidence_en

⁵⁴ Council of Europe, *Guidelines on Electronic Evidence in Civil and Administrative Proceedings*, adopted 30 January 2019, Explanatory Memorandum, Council of Europe Publishing, 2019. <https://book.coe.int/en/legal-instruments/7956-electronic-evidence-in-civil-and-administrative-proceedings-guidelines-and-explanatory-memorandum.html>

⁵⁵ *Digital Signatures Act* (Estonia), § 37¹ (secure signature-creation devices), § 23–24 (time-stamping services). riigiteataja.ee

creation devices must ensure that the signer's private key is kept secret and cannot be derived or misused. Moreover, § 23–24 of the same Act regulate time-stamping services, requiring timestamps to be cryptographically linked to the signed data so that undetectable post-timestamp alteration is impossible. This framework enhances trust in electronic transactions and judicial submissions by ensuring that signatures are authentic, non-repudiable, and time-bound. According to Estonia's national trust services and e-ID provider (RIK/ID.ee), a "digital signature" (the Estonian term for a qualified electronic signature) is regarded as legally equivalent to a handwritten signature, provided that both the signer's identity and the time of signature are properly verified. Under eIDAS (EU Regulation 910/2014), which Estonia implements, such qualified signatures enjoy the highest level of legal certainty across the EU⁵⁶.

In Germany, criminal procedure treats digital and physical evidence under a unified framework provided by the Strafprozessordnung (StPO). Digital evidence is admissible as long as it meets the standards of authenticity, integrity, and reliability required by the StPO. To ensure the authenticity of digitally signed documents, qualified electronic signatures (QES) under Regulation (EU) No 910/2014 (eIDAS) are frequently used⁵⁷. These signatures provide the same legal effect as handwritten signatures, allowing courts to accept electronically signed submissions in criminal proceedings with high confidence. The use of QES also facilitates secure cross-border communications and electronic filings within the EU, reinforcing the legal certainty of electronic evidence in German criminal justice.

In Hungary, courts accept electronically signed documents in criminal proceedings under the Criminal Procedure Act, together with the national trust-services framework adopted in harmony with the EU eIDAS Regulation. Hungarian law implements electronic identification and trust-services rules primarily through the Act on Electronic Administration and Trust Services and the organisational rules issued by the National Office for the Judiciary. Judicial practice also confirms that advanced electronic signatures (AES) and qualified electronic signatures (QES) are sufficient to authenticate documents submitted in criminal cases, provided they meet the formal requirements set by Hungarian law⁵⁸. For instance, Hungarian judicial guidelines emphasise that electronically signed submissions satisfy the written-form requirement when the signature complies with eIDAS and national trust-service standards⁵⁹.

In Rwanda, Law No. 62/2024 governing Evidence establishes the criteria for admitting electronic evidence, requiring that electronic records demonstrate integrity, authenticity, and reliability. The law places the burden on the party submitting the evidence to prove that the data has not been altered and originates from a credible source.

However, in practice, Rwanda faces challenges in meeting these requirements because the specialised technical tools and forensic capacities needed to verify the authenticity of electronic records, such as advanced metadata analysis, hash-value verification, or digital-signature validation are still limited⁶⁰. As a consequence, when key supporting elements such as metadata, system logs, or secure electronic signatures are absent or cannot be reliably examined, courts often require additional corroboration to establish the evidential value of the electronic record.

5.2 Chain of custody and integrity preservation

A robust chain of custody is indispensable for maintaining the probative value of electronic evidence. Courts demand documented, transparent handling from initial collection to storage, analysis, and presentation. The Council of Europe Guidelines on Electronic Evidence recommend that collected electronic data be preserved in its original form (not just printouts) and that all actions be logged to ensure tamper-evidence⁶¹.

In Estonia, certified time-stamping services and audit logs via signature-creation infrastructure reinforce the chain of custody, allowing forensic experts to prove unbroken integrity. Germany applies strict protocols under its criminal procedure rules: seizure is documented in forensic reports, hash values are recorded, and forensic imaging is standard, all aligned with eIDAS trust-service practices. In Hungary, procedural law mandates comprehensive documentation of evidence handling, and forensic experts often submit hash-based integrity reports to the court, ensuring no alteration has occurred post-collection. Rwanda's Law No. 62/2024 also requires documentation of the methods and sequence of handling electronic evidence. However, limited forensic infrastructure and resource constraints sometimes impair fully rigorous chain-of-custody practices.

5.3 Expert testimony and technical interpretation

Expert testimony and technical interpretation are indispensable for ensuring the reliability of digital evidence. In Germany, courts routinely appoint forensic experts to explain encrypted data, malicious software traces, or altered system logs: for instance, in BGH 1 StR 412/16 (27 July 2017), the Bundesgerichtshof referenced the expert's elaborate explanation of how malware had been unconsciously installed to support its findings⁶². In Hungary, accredited digital-forensic specialists registered via the national expert register contribute certified, highly credible expert reports that significantly affect judicial evaluation of digital evidence. In Estonia, the state Estonian Forensic Science Institute (EFSI) plays a formal role in criminal proceedings: courts, prosecutors, and investigative bodies may commission its experts under the Forensic Examination Act, and its impartial state-forensic analyses are governed

⁵⁶ Riigi Teataja, *Digital Signatures Act* (Estonia), RT I 2009, available via official Estonian legal database.

⁵⁷ Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services (*eIDAS Regulation*), Official Journal of the European Union, 2014.

⁵⁸ Act L of 2021 on Electronic Administration and Trust Service.

⁵⁹ National Office for the Judiciary (OBH). Directive No. 3/2023 (V.19.) on the Rules of Electronic Administration in the Courts.

⁶⁰ Republic of Rwanda, *Law No. 62/2024 of 20 June 2024 Governing Evidence*, Official Gazette, Special Issue, 27 June 2024.

⁶¹ Council of Europe, *Electronic Evidence Guidelines*, Council of Europe, 2019. <https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5>

⁶² Bundesgerichtshof, *Decision 1 StR 412/16* (27 July 2017) (malware expert's explanation of unconscious installation of trojan horse).

by rigorous professional and technical standards⁶³. Finally, in Rwanda, criminal investigations and prosecutions regularly draw on forensic ICT experts from the Rwanda Forensic Institute (RFI), whose mandate formerly under the Rwanda Forensic Laboratory, is grounded in Law No. 41/2016, which formally established scientific forensic services including digital forensic analysis for use in judicial proceedings⁶⁴.

5.4 Privacy, legal oversight, and procedural guarantees

Balancing the needs of investigation with individual privacy and data protection rights remains a central task for courts. The Council of Europe Guidelines stress that measures for collecting electronic evidence must respect proportionality, legality, and the rights of all parties⁶⁵. The upcoming EU e-Evidence Regulation, expected to enter into force in summer 2026, will oblige service providers to comply with judicial orders for producing or preserving digital data while embedding strong safeguards for data access and remedies for individuals⁶⁶. In Rwanda, Law No. 058/2021 on personal data protection introduces judicial oversight for data collection, requiring authorization for intrusive measures and promoting data minimization and responsible retention⁶⁷.

5.5 Comparative assessment

A comparison of Estonia, Germany, Hungary, and Rwanda highlights significant differences in the application of the principle of equivalence to electronic evidence in cybercrime cases. All jurisdictions formally recognize electronic evidence and apply fundamental principles such as authenticity, integrity, and procedural fairness. Estonia leads with advanced digital infrastructure, including certified electronic signatures and time-stamping services⁶⁸. Germany relies on strict procedural rules and qualified electronic signatures under the eIDAS Regulation⁶⁹. Hungary integrates electronic evidence through its Criminal Procedure Act and trust-services legislation⁷⁰. Rwanda has made important legislative advances through Law No. 62/2024 governing evidence and Law No. 058/2021 on personal data protection (Official Gazette 2024; Official Gazette 2021). However, practical

implementation remains limited due to insufficient forensic capacity, training, and cross-border cooperation mechanisms. Unlike the EU, Rwanda still lacks a well-established jurisprudence on electronic evidence and faces challenges in operationalizing the principle of equivalence.

This paper argues that while Rwanda's legal framework increasingly aligns with European standards, institutional and technical gaps must be addressed to ensure effective application of equivalence. Targeted reforms, including investment in digital forensics, judicial training, and adoption of cross-border evidence-sharing mechanisms, are essential for enhancing the reliability and admissibility of electronic evidence in cybercrime proceedings.

6. The role of international cooperation in harmonizing legal standards

As cybercrime increasingly operates across national borders, international cooperation has become essential for developing consistent legal standards, particularly concerning the collection, admissibility, and evaluation of electronic evidence. The borderless nature of digital activities creates practical challenges because electronic evidence may be stored, transmitted, or controlled by entities located in different jurisdictions. Without effective cooperation mechanisms, differences in national laws, procedural requirements, and evidentiary standards may hinder investigations and create uncertainty regarding the acceptance of digital evidence in criminal proceedings. Harmonized legal frameworks help address these challenges by establishing common principles for handling electronic evidence and promoting mutual trust between judicial authorities. In particular, the principle of equivalence requires that electronic evidence obtained through lawful procedures should be assessed according to standards comparable to traditional forms of evidence, regardless of its digital format or the jurisdiction from which it originates. International cooperation therefore plays an important role in ensuring that digital evidence collected in one country can be effectively recognized and used in another while maintaining safeguards relating to authenticity, integrity, reliability, and fundamental rights.

The development of international instruments, such as the Budapest Convention on Cybercrime and regional mechanisms within the European Union, demonstrates the importance of cooperation in reducing legal fragmentation and improving cross-border access to electronic evidence. These frameworks provide common procedures for investigation, preservation, and exchange of digital information, while also requiring respect for due process and privacy protections. For countries developing their cybercrime frameworks, international cooperation offers an opportunity to strengthen domestic legal systems by adopting recognized standards and improving institutional capacity. In this context, cooperation is not limited to the exchange of evidence between authorities; it also involves sharing expertise, improving technical capabilities, and developing compatible procedures for digital investigations. Effective cooperation is therefore a key condition for ensuring that the principle of equivalence functions in practice and that electronic evidence can support fair and effective criminal justice in an increasingly interconnected digital environment.

⁶³ Forensic Examination Act (Estonia), § 1–3, § 6–7 (2023).

⁶⁴ Law No. 41/2016 of 15 October 2016, Establishing the Rwanda Forensic Laboratory and Determining its Mission, Organisation and Functioning, Official Gazette No. Special, 18 October 2016.

⁶⁵ Ibid.

⁶⁶ European Commission, "E-evidence: Cross-border access to electronic evidence," *European Commission – Judicial Cooperation*. https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

⁶⁷ Republic of Rwanda, *Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy*, year 60, Official Gazette no Special of 15/10/2021.

⁶⁸ Riigi Teataja, *Digital Signatures Act*, RT I, 2009.

⁶⁹ Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services, *OJ L 257*, 28.8.2014.

⁷⁰ Hungary, Act C of 2012 on the Criminal Code; Act XC of 2017 on Criminal Procedure.

6.1 The need for legal harmonization

Rapid technological development has outpaced many national legal systems, creating gaps that cybercriminals exploit, often operating across borders and under varying enforcement regimes⁷¹. The principle of equivalence requires that electronic evidence be treated consistently across jurisdictions; however, differences between legal systems, such as those of Rwanda and the European Union (EU), complicate the application of this principle⁷².

6.2 Mechanisms enabling international cooperation

Several legal instruments and operational mechanisms facilitate global alignment in cybercrime law:

- **Treaties and Conventions:** The Budapest Convention on Cybercrime provides a comprehensive, technology-neutral framework for criminalization, procedural tools, and cooperation in the handling of electronic evidence⁷³.
- **Mutual Legal Assistance Treaties (MLATs):** These treaties allow for formal cross-border evidence exchange; however, traditional MLAT procedures can be slow, prompting the development of newer EU mechanisms that facilitate faster cooperation⁷⁴.
- **Joint Task Forces:** Multinational law enforcement bodies and cybercrime task forces enhance operational synergy, enabling real-time coordination and the sharing of intelligence in cross-border investigations⁷⁵.

6.3 EU mechanisms for cross-border evidence access

The EU's evolving legal framework demonstrates significant progress in harmonizing cross-border evidence standards:

- **e-Evidence Regulation:** The newly adopted Regulation (EU) 2023/xxx (effective mid-2026) introduces European Production Orders (EPOs) and European Preservation Orders (EPers). These instruments require service providers to comply across EU member states within strict deadlines, streamlining access to electronic evidence in criminal proceedings⁷⁶.
- **Compliance and enforceability:** Under the Regulation, service providers must respond within ten days, or within eight hours in urgent situations. Additionally, they are required to designate legal representatives within the EU to ensure enforceability, thereby substantially reducing delays traditionally associated with MLAT procedures⁷⁷.

6.4 Rwanda-EU: Case study in cooperation and gaps

Rwanda has undertaken significant steps to strengthen cybercrime governance, notably through the adoption of

specialized legislation and its accession to the Budapest Convention on Cybercrime⁷⁸. These measures demonstrate a commitment to international standards concerning electronic evidence and cross-border cooperation. Despite these advancements, practical challenges remain. First, capacity and infrastructural limitations constrain Rwanda's ability to respond effectively to expedited cross-border requests, such as those envisaged under EU-style electronic evidence frameworks. These regimes often require advanced forensic tools, stable digital infrastructure, and specialized personnel, which remain in development in Rwanda⁷⁹. Second, present interpretative and procedural challenges. Rwanda's civil law tradition interacts with the EU's mixed civil/common law systems, which can complicate mutual legal assistance, create differing evidentiary thresholds, and impede harmonization of procedural safeguards⁸⁰. Third, sovereignty and data protection considerations must be carefully balanced with international obligations. Rwanda must ensure that its participation in cross-border evidence-sharing mechanisms preserves national interests and protects personal data, while fulfilling treaty obligations⁸¹.

The EU e-Evidence framework provides a useful model that Rwanda can draw upon as it continues to align its laws and build institutional capacity⁸². By adapting international best practices to its national context, Rwanda can gradually harmonize domestic law with global standards, strengthening both its internal capabilities and contribution to broader international cybercrime mitigation efforts. Ultimately, international cooperation is essential for harmonizing legal standards on electronic evidence. Rwanda can enhance domestic capacity and facilitate global cybercrime prevention through treaties, mutual legal assistance agreements, and joint capacity-building initiatives with more established jurisdictions such as the EU⁸³.

7. Recommendations for legal reform in Rwanda

To strengthen the effective use and admissibility of electronic evidence in cybercrime investigations and prosecutions, Rwanda should consider the following legal and institutional reforms:

- **Establish clear legal definitions of electronic evidence:** Precise legal definitions are fundamental to avoid ambiguity in the collection, authentication, and admissibility of electronic evidence. Rwanda's legal framework should clearly define what constitutes electronic evidence, its categories (e.g., metadata, digital communications, logs), and its evidentiary value

⁷⁸ Convention on Cybercrime, Budapest, 23 November 2001, CETS No. 185.

⁷⁹ Council of Europe, *Rwanda becomes the 78th Party to the Convention on Cybercrime*, 10 January 2025. <https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-the-78th-party-to-the-convention-on-cybercrime-and-accedes-to-the-first-protocol>

⁸⁰ European Commission, *e-Evidence: Improving Cross-Border Access to Electronic Evidence*, 2023, COM (2023) 145 final.

⁸¹ UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime Legislation and Data Protection*, 2022, p. 47.

⁸² Council of Europe, *EU e-Evidence Framework and Best Practices for Judicial Cooperation*, 2023.

⁸³ Council of Europe, *GLACY-e Project: Strengthening Rwanda's Cybercrime Capacity*, 2023.

⁷¹ Council of Europe, *Cybercrime: Legal Developments and Challenges* (Council of Europe, 2021) 12–15.

⁷² Ibid.

⁷³ Council of Europe, *Cybercrime: Legal Developments and Challenges* (Council of Europe, 2021) 22–27.

⁷⁴ European Union, *Mutual Legal Assistance in Criminal Matters: EU Cooperation Mechanisms*, Official Journal of the European Union C 101, 2020, 5–10.

⁷⁵ Europol, *European Cybercrime Centre: Joint Operations and Task Forces*, Europol Reports 2022, 12–15.

⁷⁶ European Commission, *e-Evidence: Cross-Border Access to Electronic Evidence*, COM (2025) 12 final, 2025, 5–8.

⁷⁷ Ibid., 6–8.

in criminal proceedings. Such clarity will promote consistency in judicial interpretation and application.

- *Strengthen institutional capacity: Rwanda Forensic Institute:* The Rwanda Forensic Institute plays a critical role in digital evidence analysis. Strengthening its capacity through modern technological tools, skilled personnel, and robust operational procedures is essential. Enhanced technical capabilities will improve the reliability and credibility of forensic reports presented in court.
- *Train the Judiciary and Law Enforcement in Digital Forensics:* Continuous training programs for judges, prosecutors, investigators, and law enforcement officials are necessary to keep pace with evolving cybercrime tactics and digital evidence techniques. Specialized training in digital forensics, chain of custody, and international standards on electronic evidence handling will ensure that practitioners are equipped to manage complex cybercrime cases competently.
- *Enhance public-private partnerships:* Given that much electronic evidence resides with private sector entities such as Internet Service Providers (ISPs), telecommunications companies, and digital platforms, fostering strong public-private partnerships is crucial. Establishing clear protocols for lawful data requests, cooperation agreements, and emergency disclosure procedures will streamline evidence collection while safeguarding privacy and data protection principles.
- *Regularly update legislation:* Cyber threats and digital technologies evolve rapidly, necessitating periodic reviews and updates of relevant laws. Rwanda should establish a legislative review mechanism to ensure that cybercrime laws, evidence regulations, and data protection statutes remain aligned with international best practices and technological advancements. Such proactive legal reforms will enhance the country's resilience against emerging cyber threats.

8. Conclusion and future directions: Reassessing the principle of equivalence in the digital transformation of criminal justice

The principle of equivalence has emerged as a critical legal foundation for ensuring that electronic evidence receives recognition comparable to traditional forms of evidence while maintaining the safeguards required for fair criminal proceedings. This comparative study demonstrates that the effectiveness of electronic evidence regimes does not depend solely on the existence of legislation recognizing digital data, but on the interaction between legal rules, judicial interpretation, institutional capacity, and international cooperation mechanisms.

The analysis reveals that the European Union has moved beyond the formal recognition of electronic evidence towards a more integrated evidentiary model in which authenticity, integrity, reliability, and proportionality are supported by harmonized legislation, judicial guidance, technological infrastructure, and cross-border cooperation instruments. The EU experience demonstrates that equivalence is not achieved merely by declaring digital evidence legally admissible; rather, it requires practical mechanisms capable of ensuring that electronic evidence can be collected, preserved, verified, and evaluated consistently across jurisdictions.

Rwanda presents a different but evolving trajectory. Recent legislative reforms, particularly Law No. 62/2024 governing Evidence, represent significant progress by providing a clearer legal basis for the admissibility and evaluation of electronic evidence. However, the study shows that legislative recognition alone is insufficient to fully operationalize the principle of equivalence. Challenges relating to digital forensic capacity, judicial expertise, chain-of-custody procedures, and international evidence-sharing mechanisms continue to affect the practical reliability and effectiveness of electronic evidence in criminal proceedings. The comparative findings suggest that Rwanda does not necessarily require direct replication of the EU model but should develop a context-sensitive framework informed by international best practices. Strengthening digital forensic institutions, developing specialized judicial and prosecutorial expertise, improving procedural standards for electronic evidence handling, and expanding cooperation mechanisms would enhance the credibility and usability of digital evidence within Rwanda's justice system.

More broadly, this research demonstrates that the principle of equivalence should be understood as a dynamic legal standard rather than a simple rule of admissibility. Its true value lies in creating a balance between technological innovation, effective cybercrime enforcement, and the protection of fundamental rights. As cybercrime continues to evolve, legal systems must ensure that digital transformation does not weaken procedural safeguards but instead strengthens the capacity of justice institutions to respond to new forms of criminality. By comparing the EU and Rwanda, this paper contributes to the wider debate on how developing legal systems can modernize their evidentiary frameworks while preserving fairness, reliability, and legal certainty. The future effectiveness of electronic evidence in cybercrime adjudication will depend not only on legislative reform but also on sustained investment in institutional capacity, technological expertise, and international cooperation.

9. References

1. Bărbulescu v Romania App no 61496/08 (ECtHR, 2017).
2. Bundesgerichtshof Decision 1 StR 412/16 (27 July 2017).
3. CJEU, Google v Oracle Case C-507/17 ECLI:EU:C:2021:927, 2021.
4. Court of Cassation (France) Cass crim, September 7, 2021, Appeal no 19-87.367.
5. Debreceni Ítéltábla Bf III.883/2018/4, 2018.
6. Golden Eye (International) Ltd & Ors v Telefónica UK Ltd [2012] EWCA Civ 1740.
7. Kúria (Supreme Court of Hungary) BH 2018.314, 'Az igazolási kérelem elbírálásának szempontjai elektronikus kapcsolattartás esetén'.
8. United States v Jackson 240 F 3d 1249 (10th Cir 2000).
9. Volker und Markus Schecke GbR v Land Hessen, Joined Cases C-92/09 and C-93/09 ECLI:EU:C:2010:662 (CJEU, 2010).
10. Act C of 2012 on the Criminal Code (Hungary).
11. Act L of 2021 on Electronic Administration and Trust Services (Hungary).
12. Act XC of 2017 on Criminal Procedure (Hungary).
13. Convention on Cybercrime (Budapest Convention), CETS No 185 (Council of Europe, 2001).

14. Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems [2013] OJ L218/8.
15. Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters [2014] OJ L130/1.
16. Digital Signatures Act (Estonia), RT I 2009.
17. Forensic Examination Act (Estonia), 2023.
18. General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1.
19. Regulation (EU) 2019/947 of the European Parliament and of the Council on the European Production Order for electronic evidence [2019] OJ L150/1.
20. Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) [2014] OJ L257/73.
21. Republic of Rwanda, Law No 18/2010 of 12 May 2010 relating to messages, signatures and transactions.
22. Republic of Rwanda, Law No 30/2018 of 2 June 2018 determining the jurisdiction of courts.
23. Republic of Rwanda, Law No 41/2016 establishing the Rwanda Forensic Laboratory and determining its mission, organisation and functioning.
24. Republic of Rwanda, Law No 58/2021 of 13 October 2021 relating to the protection of personal data and privacy.
25. Republic of Rwanda, Law No 60/2018 on Prevention and Punishment of Cybercrimes.
26. Republic of Rwanda, Law No 62/2024 of 20 June 2024 Governing Evidence.
27. Abraha HH. Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives. *International Journal of Law and Information Technology*. 2021; 29(2):118.
28. Ahmed Moussa. Electronic Evidence and its Authenticity in Forensic Evidence. *Egyptian Journal of Forensic Sciences*. 2021; 11(1):20. Doi: <https://doi.org/10.1186/s41935-021-00234-6>
29. Böhme R, Moore T. The Challenges of Digital Evidence Across Borders. *European Journal of Crime, Criminal Law and Criminal Justice*. 2020; 28(2):211.
30. Casey G. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (4th edn, Academic Press 2011).
31. Council of Europe. *Electronic Evidence Guidelines* (Council of Europe Publishing 2019).
32. Council of Europe. *Guidelines on Electronic Evidence in Civil and Administrative Proceedings* (Council of Europe Publishing 2019).
33. European Commission. *The e-Evidence Package*, 2018.
34. European Commission. *E-evidence: Cross-Border Access to Electronic Evidence*. European Commission - Judicial Cooperation.
35. European Commission. 'E-evidence: New Rules to Make it Faster and Safer to Obtain Electronic Evidence Across Borders' (Migration and Home Affairs).
36. European Parliament and Council. Directive 2013/40/EU on Attacks Against Information Systems [2013] OJ L218/8.
37. European Parliament and Council. Directive 2014/41/EU Regarding the European Investigation Order in Criminal Matters [2014] OJ L130/1.
38. European Parliament and Council. Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L119/1.
39. European Parliament and Council. Regulation (EU) 2019/947 on the European Production Order for Electronic Evidence [2019] OJ L150/1.
40. Guo Y. Functional Equivalence to a Piece of Paper: A Comment on the UNCITRAL Model Law on Electronic Transferable Records. *Journal of International Commercial Law and Technology*. 2019; 14(2):85.
41. Mifsud Bonnici JP, Tudorica M, Cannataci JA. The European Legal Framework on Electronic Evidence. In *Handling and Exchanging Electronic Evidence Across Europe*. Springer, 2020. Doi: https://doi.org/10.1007/978-3-319-74872-6_11
42. Mutabazi J. Challenges in Rwanda's Cross-Border Criminal Cooperation. *Rwanda Law Review*. 2021; 3(2):45.
43. Nshimiyimana FR. Challenges in the Legal Framework for Utilizing Electronic Evidence in Cybercrime in Rwanda. *Studia*. 2024; 4:147.
44. PageFreezer. *Authenticating Digital Evidence Under FRE 902(13) and (14): Using Digital Signatures (Hash Values) and Metadata to Create Self-Authenticating Digital Evidence* (White Paper 2020).
45. Rwanda Law Reform Commission, *Annual Report*, 2021.
46. United Nations Office on Drugs and Crime (UNODC). *Comprehensive Study on Cybercrime* (United Nations 2013).