Journal of Cyberspace Studies
eISSN: 2588-5502
http://jcss.ut.ac.ir
University of Tehran

Dual criminality in the digital age: Strengthening cross-border cooperation in cybercrime investigations

Nshimiyimana Francois Regis
Judge (on academic leave), Rwandan Judiciary, Researcher on Electronic Evidence in Cybercrime, Károli Gáspár University of the Reformed Church, Hungary. (✉regisnshimiye82@gmail.com, https://orcid.org/0009-0001-4723-1485)

Article Info

Original Article

Main Object: Law

Received: 14 September 2025
Revised: 25 February 2026
Accepted: 25 February 2026
Published online: 05 April 2026

Keywords:
cross-border cooperation,
cybercrime,
dual criminality,
electronic evidence,
mutual legal assistance.

Abstract

Background: The principle of dual criminality, which requires an act to be criminalized in both the requesting and requested states, is a cornerstone of mutual legal assistance. However, the rise of cybercrime, characterized by its borderless nature and reliance on perishable electronic evidence, has created significant challenges. Divergent legal definitions, procedural variations, and evidentiary standards frequently delay or obstruct cross-border investigations.
Aims: This paper examines the limitations of dual criminality in cybercrime investigations and explores how technological advancements and inconsistent domestic frameworks affect international cooperation.
Methodology: A comparative legal analysis is employed, drawing on the legal systems and practices of Rwanda, Germany, Estonia, and Hungary. These jurisdictions were selected to represent non-EU and EU states with diverse legal traditions. The study also evaluates key international instruments, including the Budapest Convention and its Additional Protocols, alongside mechanisms such as the European Investigation Order.
Discussion: Findings reveal structural and procedural barriers, such as inconsistent offence definitions, jurisdictional conflicts, and inadequate technical capacity, which hinder timely and lawful evidence sharing. These gaps undermine trust and efficiency in cooperation.
Conclusion: The paper recommends harmonizing cybercrime definitions, adopting technology-adapted dual criminality assessments, implementing fast-track evidence-sharing mechanisms, and strengthening mutual trust through capacity-building and rights-protection measures. These steps aim to reconcile dual criminality with the urgent need for efficient and rights-compliant international collaboration.

Cite this article: Regis NF. (2026). "Dual criminality in the digital age: Strengthening cross-border cooperation in cybercrime investigations". *Cyberspace Studies*. 10(2): 637-661. doi: https://doi.org/10.22059/jcss.2026.402346.1180.

Website: https://jcss.ut.ac.ir/| Email: jcss@ut.ac.ir |
EISSN: 2588-5502
Publisher: University of Tehran

Cyberspace Studies, Vol 10, No 2, July 2026

1. Introduction

The accelerated growth of the digital landscape has fundamentally altered the character of criminal conduct, permitting offences to be executed instantaneously across national boundaries. Cybercrime, encompassing advanced ransomware operations and unlawful data interception, has emerged as a significant global security concern that surpasses conventional jurisdictional limits. The effective investigation and prosecution of such offences frequently necessitate transnational collaboration, as evidence, offenders, and victims are often dispersed across multiple legal systems (Singh, 2024). This cooperation is generally operationalised through mutual legal assistance treaties (MLATs), regional legal instruments, and multilateral agreements, most prominently the Budapest Convention on Cybercrime (Council of Europe, 2001). Nevertheless, the principle of dual criminality continues to function as a central— though occasionally contentious— precondition for facilitating such international cooperation.

Dual criminality, the principle that the act in question must be criminalized in both the requesting and requested state, has long been a cornerstone of *international criminal law* and extradition practice (Plachta, 1989). It functions as a safeguard against arbitrary interference in the domestic legal order of the requested state, ensuring mutual respect for national sovereignty and legal diversity (Boister, 2021). In traditional contexts, dual criminality has not posed insurmountable obstacles; most serious crimes such as murder, fraud, or drug trafficking are recognized as offences across legal systems.

Cybercrime, however, generates a series of complex challenges in the application of the dual criminality requirement. First, the definitions and substantive scope of cyber offences diverge significantly across jurisdictions. Second, the rate at which domestic legislation adapts to technological developments varies markedly. Jurisdictions possessing more advanced cybercrime frameworks may submit cooperation requests that less technologically updated legal systems lack the normative capacity to fulfil (Kulesza, 2019a). Third, questions of territoriality—particularly in matters involving data stored within cloud infrastructures distributed across multiple states—complicate the determination of the locus delicti, that is, the jurisdiction in which the offence is considered to have been committed (Svantesson, 2017).

From a *practical enforcement perspective*, these challenges can result in delays, refusals, or incomplete cooperation in cybercrime investigations. For example, suppose a Rwandan investigation into phishing attacks seeks electronic evidence from Germany. In that case, the request may be denied if Germany does not criminalize certain preparatory acts in the same way as Rwandan law. Similar obstacles can arise in the context of *Estonia's advanced cybercrime framework* when interacting with countries whose legislation does not explicitly cover offences such as denial-of-service attacks (Ragni, 2023).

Hungary's recent amendments to its criminal code in line with the Budapest Convention, further highlight the disparities between jurisdictions that have modernized their legal frameworks and those that have not (Hungarian Ministry of Justice, 2021).

This paper seeks to *critically analyze* the operation of the dual criminality principle in cybercrime cases, drawing on comparative examples from *Rwanda*, *Germany, Estonia, and Hungary*. The research aims are threefold:

- To identify how differing definitions of cyber offences impact cross-border cooperation.
- To assess whether the dual criminality principle, as currently applied, is fit for purpose in the digital age.
- To propose *practical reforms*, both legislative and procedural, that could strengthen international cooperation without undermining fundamental legal safeguards.

This study adopts a comparative legal methodology, integrating doctrinal examination of statutory frameworks, international instruments, judicial decisions, and practical perspectives derived from law enforcement cooperation. The analysis is grounded in a review of domestic cybercrime legislation across the four selected jurisdictions, alongside relevant provisions of the Budapest Convention on Cybercrime and its associated Protocols, as well as documented operational challenges encountered by practitioners involved in cross-border investigations.

2. Literature review

The principle of dual criminality remains a cornerstone of mutual legal assistance (MLA) in criminal matters, but the borderless nature of cybercrime and the volatility of electronic evidence have created significant challenges in its application (Singh, 2024). One major obstacle is the lack of uniformity in cybercrime legislation across jurisdictions. While Germany may define a specific act as computer fraud, Rwanda may treat it as unauthorized access, and Estonia as cyber-extortion. Such discrepancies require prosecutors to undertake complex equivalency analyses, which slow investigations. Edelman (2020) argue for greater harmonization of offence definitions to enhance predictability and streamline legal processes.

The Budapest Convention on Cybercrime has been widely recognized as a key instrument for harmonizing cybercrime definitions and enabling cross-border evidence-sharing (Council of Europe, 2001). Its provisions, notably on illegal access, data interference, and expedited preservation of electronic evidence, have reduced uncertainty in some contexts (Bacher et al., 2021). However, implementation remains uneven, particularly in jurisdictions with limited technical capacity or divergent legal traditions. Comparative research further

reveals differences between EU and non-EU approaches to electronic evidence (Juszczak & Sason, 2023). The EU's European Investigation Order (EIO) facilitates streamlined cooperation, while non-EU states often face legal and procedural barriers rooted in dual criminality requirements. High-profile cases, such as the extradition proceedings involving Huawei's CFO Meng Wanzhou, illustrate the complexities and delays these requirements can cause (Cao, 2025). Such disparities underscore the need for a more harmonized global framework that balances effective enforcement with respect for sovereignty (Coupland, 2020).

Despite these developments, significant gaps remain in the literature. Using internete and social media has been continuously on the raise (see for example Shahghasemi et al., 2025) and the need for advanced research on crimes that happen in this sphere is undeniable. Few studies address African–EU cooperation on cybercrime, particularly regarding Rwanda, and limited attention has been paid to emerging threats such as AI-enabled fraud and ransomware in the context of dual criminality (Adeniran et al., 2024). Addressing these gaps is critical to ensuring timely, rights-compliant cross-border investigations in an increasingly digital world (Kurshan et al., 2025). In the view of this paper, this approach contrasts sharply with Rwanda's current framework, which, although substantially aligned with the Budapest Convention, still lacks explicit provisions for emerging cybercrime categories such as ransomware-as-a-service and deepfake-related offences. This gap makes cooperation with technologically advanced jurisdictions more complex and less efficient.

3. Conceptual and legal foundations of dual criminality in cybercrime

3.1. Definition and historical role of the dual criminality principle

The principle of dual criminality mandates that an act must be considered a criminal offence in both the requesting and requested jurisdictions for extradition or mutual legal assistance (MLA) to be granted. This principle serves as a safeguard against the enforcement of foreign laws that may be incompatible with domestic legal norms, thereby protecting national sovereignty and legal autonomy (Council of Europe, 2001, art. 25).

Historically, dual criminality emerged as a fundamental requirement in international legal cooperation, particularly in the 19th century, to ensure that states would not be compelled to extradite individuals for acts that were not criminal under their laws (United Nations, 2000, art. 16). This principle has been enshrined in various international treaties and conventions, reflecting its importance in maintaining the integrity of domestic legal systems while facilitating international cooperation.

3.2. Legal rationale for dual criminality in MLA and extradition

The legal rationale for dual criminality in MLA and extradition is multifaceted:

- **Protection of sovereignty.** Dual criminality ensures that a state is not obligated to enforce foreign laws that may conflict with its legal principles, thereby preserving its sovereignty (Council of the European Union, 2002).
- **Fairness and proportionality.** It guarantees that individuals are not subjected to prosecution or punishment for acts that are not criminal under the laws of the jurisdiction in which they are located (European Parliament & Council, 2014).
- **Legal certainty.** The principle provides a clear and objective criterion for determining the legitimacy of international cooperation requests, reducing the potential for arbitrary or politically motivated actions (European Parliament & Council, 2023).

In the context of cybercrime, where offences often transcend national borders and may not be uniformly defined across jurisdictions, dual criminality serves as a critical mechanism to ensure that international cooperation is both legally justified and equitable (Germany, Federal Court of Justice, 2015).

3.3. Treatment under international and regional instruments

International and regional legal instruments provide frameworks for applying the dual criminality principle in cybercrime cases. These instruments aim to strike a balance between effective cross-border cooperation and respect for national legal systems, ensuring that assistance is granted only for conduct recognized as criminal in both jurisdictions.

- **Budapest Convention on Cybercrime.** Article 25 of the Convention expressly addresses the principle of dual criminality, providing that mutual legal assistance may be made contingent upon the fulfilment of this requirement. Nevertheless, it adopts a flexible approach by permitting assistance even where the requested state does not classify the offence under an identical legal denomination or employ the same terminology as the requesting state, provided that the underlying conduct constitutes a criminal offence in both jurisdictions (Bacher et al., 2021).
- **United Nations Convention against Transnational Organized Crime (UNTOC).** Article 16 of the UNTOC incorporates the dual criminality principle, requiring that the offence for which extradition is requested must be punishable under the laws of both the requesting and requested states (Tikk & Kaska, 2010).

- **European Union instruments.** The European Union has developed a range of legal instruments to facilitate judicial cooperation among its member states, particularly in criminal matters. These instruments aim to streamline cross-border investigations and prosecutions by reducing procedural barriers and enhancing mutual trust between national authorities. Central to this framework are the European Arrest Warrant (EAW) and the European Investigation Order (EIO), which both address the principle of dual criminality in distinctive ways. While the EAW provides for limited or conditional abolition of dual criminality for serious offences, including cybercrime, the EIO emphasizes practical cooperation in investigative measures, focusing on the substance of the conduct rather than strict formal classification. These instruments exemplify the EU's flexible approach to cross-border criminal justice, balancing efficiency with respect for member states' legal systems.
    - **European Arrest Warrant (EAW).** Under the EAW framework, dual criminality is generally abolished for offences listed in Article 2(2) of Framework Decision 2002/584/JHA. This includes serious crimes such as cybercrime, provided the offence is punishable by a custodial sentence of at least three years in the issuing member state.[1]
    - **European Investigation Order (EIO).** The EIO Directive (2014/41/EU) allows for the execution of investigative measures without prior recognition of the offence in the executing state, provided the conduct would constitute an offence under the law of the executing state had it occurred domestically.[2]

3.4. Distinction between strict and flexible application of dual criminality

The principle of dual criminality plays a pivotal role in facilitating international legal cooperation, particularly in extradition and mutual legal assistance. Its application, however, is not uniform across jurisdictions. Depending on the legal framework and practical considerations, dual criminality can be applied in either a strict or flexible manner. Understanding these two approaches is essential, as

1. Under the European Arrest Warrant (EAW) framework, dual criminality is generally abolished for the offences listed in Article 2(2) of Council Framework Decision 2002/584/JHA, including serious crimes such as cybercrime punishable by at least three years' imprisonment in the issuing member state (Council of the European Union, 2002).
2. The European Investigation Order (EIO) Directive (2014/41/EU) permits investigative measures to be executed in another member state without prior recognition of the offence, as long as the conduct would constitute a criminal offence under the executing state's domestic law if it had occurred there (European Parliament & Council, 2014).

they determine the extent to which states can collaborate in prosecuting cross-border offences, especially in the rapidly evolving domain of cybercrime.

- **Strict application.** Requires the offence to be identical in both jurisdictions, in terms of legal classification and terminology. This ensures that states only cooperate in cases where the conduct is unequivocally criminal under their laws (United Nations General Assembly, 2022).
- **Flexible application.** Focuses on the substance of the conduct rather than its formal classification. Cooperation is allowed even if the offence is not identically defined in both jurisdictions, provided the conduct would be criminal under the laws of both states. This approach is particularly important in cybercrime, where technological advancements often outpace legislative processes (ibid.)

4. Methodology

This study employs a comparative legal analysis methodology, integrating doctrinal examination with a jurisdiction-comparative framework. The doctrinal component involves systematic analysis of primary legal sources across four selected jurisdictions— Rwanda, Germany, Estonia, and Hungary— including domestic cybercrime statutes, criminal procedure codes, and judicial decisions. These national sources are examined alongside key international and regional instruments, principally the Budapest Convention on Cybercrime (ETS No. 185) and its Second Additional Protocol (CETS No. 224), the European Arrest Warrant Framework Decision (2002/584/JHA), the European Investigation Order Directive (2014/41/EU), and the EU e-Evidence Regulation (2023/1543). The analysis also draws on policy documents, implementation reports, and operational guidance issued by institutions such as Eurojust, Europol, the Council of Europe Cybercrime Programme Office, and the European Judicial Network. The four jurisdictions were deliberately selected to maximize analytical contrast: Rwanda represents a non-EU state with a developing but rapidly evolving cybercrime framework and recent Budapest Convention accession; Germany exemplifies a civil-law EU Member State with a rigorous legality culture and exacting dual-criminality scrutiny; Estonia offers the perspective of a digitally mature EU state that has institutionalized rapid-response cyber cooperation since the 2007 distributed denial-of-service attacks; and Hungary illustrates a civil-law EU Member State whose procedural reforms and Budapest-aligned codification present a distinct model of legislative adaptation.

The comparative dimension of the study is structured around five analytical criteria applied consistently across all four jurisdictions: (i) the degree of alignment between domestic offence definitions and the substantive categories prescribed by the Budapest Convention; (ii) the

existence of legislative gaps with respect to emerging forms of cybercrime, such as ransomware-as-a-service operations, deepfake-facilitated fraud, and AI-enabled offences (Habib Zadeh Khiyaban & Sabbar, 2022); (iii) the practical application of the dual criminality requirement in mutual legal assistance and extradition proceedings; (iv) the admissibility and evidentiary treatment of electronically gathered foreign evidence; and (v) the extent to which mutual recognition instruments, including the EIO and the forthcoming e-Evidence Regulation, are operationalized to accelerate cross-border evidence flows. This framework enables systematic cross-jurisdictional comparison while remaining sensitive to the specific procedural and constitutional contexts of each legal system. It is important to acknowledge the study's limitations in this regard: the analysis is primarily doctrinal and does not incorporate empirical data derived from law enforcement casework or practitioner surveys.

5. Discussion

5.1. Current legal issues in cybercrime and dual criminality

5.1.1. Mismatch of national cybercrime laws

A central difficulty in international cybercrime investigations lies in the divergence of national legal frameworks. States differ considerably in their definitions of offences such as illegal access, data interference, and computer-related fraud. For example, the Budapest Convention on Cybercrime defines illegal access as the unauthorised entry into a computer system (Eurojust & Europol, 2019). However, a number of jurisdictions continue to lack a precise statutory formulation of this offence, thereby complicating cross-border cooperation (Wu, 2021).

Emerging forms of criminality— such as attacks targeting cloud infrastructures or ransomware-as-a-service (RaaS) models— are likewise not criminalised in a uniform manner. In Rwanda, for instance, domestic legislation criminalises unauthorised access and data interference but does not expressly address RaaS operations or identity fraud facilitated through deepfake technologies (Rwanda, 2018). By contrast, Member States of the European Union, including Germanyand Hungary, have begun incorporating such conduct into their criminal codes through amendments to existing cybercrime legislation (European Commission, 2024). This normative asymmetry generates obstacles in satisfying the dual criminality requirement, as conduct constituting a criminal offence in one jurisdiction may not be recognised as such in another. The resulting misalignment can delay mutual legal assistance (MLA) procedures and hinder the timely execution of investigative measures (Council of Europe, 2013).

5.1.2. Emerging digital threats and legal adaptation

The pace of technological innovation in cyberactivities including cybercrime often outstrips legislative responses (Shahghasemi, 2016).

AI-assisted fraud, deepfakes, ransomware campaigns, and crypto laundering illustrate threats that bypass traditional offence lists (Kurshan et al., 2025). For example, the WannaCry ransomware attack of 2017 affected over 200,000 computers globally, exploiting vulnerabilities that were not addressed in some national legal codes at the time (Kao et al., 2019). Similarly, AI-generated deepfakes are increasingly used for financial fraud or political manipulation, yet many jurisdictions lack explicit statutes criminalizing the creation or distribution of such material (Kaushik et al., 2024). Since AI technology is increasingly capable of generating realistic content and images (Salehi et al., 2025), this legal lag not only complicates prosecution but also raises evidential questions regarding intent, authorship, and admissibility of AI-generated digital evidence.

5.1.3. Procedural vs. substantive law conflicts

One of the pressing challenges in the admissibility of electronic evidence is the tension between procedural and substantive law. Substantive law defines whether a digital act constitutes a criminal offence, while procedural law regulates how evidence relating to that offence is collected, preserved, and presented before courts. In practice, divergences between jurisdictions are profound. For instance, in Ireland, unauthorized data access can be pursued under the *Data Protection Act 2018* primarily as a breach of data protection obligations, often resulting in civil or administrative sanctions (Data Protection Act, 2018). By contrast, Hungary criminalizes the same conduct under its *Criminal Code (Act C of 2012)*, treating unauthorized access to information systems as a criminal offence with possible custodial penalties (Act C of 2012 on the Criminal Code, Hungary). These substantive differences complicate mutual legal assistance requests (MLAs), as one jurisdiction may view the alleged conduct as non-criminal, thus failing the dual-criminality test.

Procedural law adds another layer of complexity. While some states permit the covert collection of digital evidence without prior judicial authorization in urgent situations, others require strict judicial oversight at every stage (Sheppard, 2020). This divergence means that evidence lawfully collected abroad may be deemed inadmissible in the requesting state. An illustrative example is *R v Baines* [2019] UKSC 14, where the UK Supreme Court partially excluded electronic evidence obtained from servers abroad due to procedural irregularities in the requesting state (R v Baines, 2019). Such conflicts underline the necessity of harmonized procedural safeguards, or at a minimum, bilateral agreements that establish mutual recognition of investigative standards (Bąkowski, 2023).

5.1.4. Sovereignty vs. rapid evidence collection

Another fundamental issue is the conflict between state sovereignty and

the practical need for rapid evidence collection in cybercrime investigations. Cybercrimes often involve data stored across multiple jurisdictions, sometimes in real-time environments where evidence can be deleted or altered within seconds. Traditional mechanisms such as mutual legal assistance treaties (MLATs) are notoriously slow, sometimes taking months to process (Council of Europe, 2021). This delay undermines effective enforcement and increases the risk of impunity for offenders. From a sovereignty perspective, states are reluctant to permit direct access by foreign authorities to data stored within their territory, viewing such acts as a violation of territorial integrity (Gercke, 2012). Yet from an enforcement standpoint, delays in securing evidence often make prosecution impossible. The Second Additional Protocol to the Budapest Convention attempts to strike a balance by introducing expedited procedures for cross-border access to electronic evidence, while still requiring certain safeguards to protect sovereignty (Council of Europe, 2022).

A practical tension emerges: if investigators wait for MLA procedures, the evidence may disappear; if they act unilaterally, they risk violating international law and rendering the evidence inadmissible in court (Milanovic & Schmitt, 2020). Thus, developing clear frameworks for direct cooperation between service providers and law enforcement agencies, alongside bilateral or multilateral treaties, is critical to reconciling sovereignty concerns with the realities of digital investigations (Kulesza, 2019b).

5.2. Case study analysis: Rwanda, Germany, Estonia, and Hungary

This section compares four jurisdictions across five practical dimensions: (i) how closely their offence definitions align with the Budapest Convention (illegal access, interception, data/system interference, computer-related fraud); (ii) whether gaps remain (especially for novel phenomena); (iii) how dual-criminality is applied in practice; (iv) the admissibility and handling of foreign-gathered electronic evidence; and (v) how far mutual-recognition instruments are leveraged to accelerate cross-border evidence flows. Where relevant, we connect national practice to the EU's mutual recognition acquis, primarily the European Investigation Order (EIO) and the new e-Evidence framework, because these instruments now shape day-to-day cooperation on subscriber, traffic, and content data across (and increasingly beyond) the EU.[1]

1. This section compares four jurisdictions across five practical dimensions of cybercrime law, including offence alignment with the Budapest Convention, dual criminality, and cross-border evidence handling. For offence definitions, see Council of Europe (2001), Art. 2 (Illegal access, interception, data/system interference, computer-related fraud).

5.2.1. Rwanda: Partial alignment with the Budapest Convention; maturing cooperation posture

Rwanda has experienced a notable surge in cybercrime activities, particularly during the COVID-19 lockdown, where incidents increased by 72% (Rwanda Investigation Bureau, 2020). In 2020, 141 cyber fraud cases were reported, involving approximately RWF 371 million; of this, RWF 280 million remained unrecovered (ibid). The Rwanda Investigation Bureau (RIB) has been actively involved in combating these crimes, with a dedicated Cybercrime Investigation Division established to address the growing threat.

To bolster its cybersecurity framework, Rwanda established the National Cybersecurity Authority (NCSA) in 2017, tasked with coordinating national efforts to protect critical information infrastructure and respond to cyber incidents (Republic of Rwanda, 2017). Additionally, the National Cybersecurity Strategy outlines strategic pillars to promote cyber resilience, build the cybersecurity industry, and enhance cooperation and collaboration. In response to the escalating cyber threats, Rwanda has also inaugurated a regional cybercrime investigation center, serving as a training hub for mobile and computer forensics, malware analysis, and cyber investigations (ibid).

Rwanda's *Law No. 60/2018 on the Prevention and Punishment of Cybercrimes* tracks the Budapest Convention's core offence families. Chapter IV criminalizes *unauthorized access* (Art 16), *unlawful interception* (Art 17), and *interference with data/systems* with gradations tied to intent and harm; the statute also contains computer-related fraud, device/offence-preparation, and payment-card offences. The text expressly authorizes forensic methods and court-ordered preservation, signaling awareness of digital-evidence workflows (Rwanda, 2018). In January 2025, Rwanda acceded to the Budapest Convention, joining the 24/7 Network and committing to procedural cooperation standards designed to reduce friction for preservation and disclosure requests (Council of Europe, 2025).

While the 2018 law is broadly consonant with Budapest's Article 2–6 offences, it does not expressly legislate for some next-generation behaviors (e.g., deep fake-specific misuse or platform-as-a-service criminal facilitation). Those behaviors are typically pursued via general fraud, forgery, or privacy offences, which can be serviceable but sometimes complicate dual-criminality analysis where partners require a like-for-like cyber-offence. Before 2025, the absence of Convention party status often meant heavier reliance on slower mutual legal assistance channels; accession should improve timeliness for basic subscriber/IP attribution via 24/7 requests and expedited preservation under the Convention's procedural toolkit (European Parliament & Council, 2014).

5.2.2. Germany: Strong harmonization; exacting legality and dual-criminality controls

Germany's StGB has long contained a granular cybercrime chapter that closely mirrors Budapest and EU law: *data espionage/illegal access* (§ 202a), *interception of data* (§ 202b), *preparation of offences/tools* (§ 202c), *data alteration* (§ 303a), *computer sabotage* (§ 303b), and *computer fraud* (§ 263a). These provisions, frequently updated in light of EU instruments, provide clear anchors for dual-criminality assessments and prosecutorial charging. [1] Dual-criminality and cooperation. For international cooperation measures, Germany's Act on International Mutual Assistance in Criminal Matters (IRG) typically requires dual criminality unless a specific exception applies (and subject to proportionality and data-protection safeguards). This underpins a comparatively strict legality filter on incoming requests, including some EIO-executed measures where German authorities assess availability/equivalence under domestic law. [2] The Commission's EIO implementation report notes that, across Member States, variability in transposition and grounds for refusal continues to generate friction, one reason the EU has complemented the EIO with the direct-to-provider e-Evidence Regulation (European Parliament & Council, 2023).

Admissibility of foreign e-evidence (EncroChat). German courts have wrestled with cross-border law-enforcement hacking and the downstream use of bulk chat data acquired abroad. In 2 BvR 558/22 (2023), the Federal Constitutional Court affirmed that EncroChat data obtained by French authorities and shared via mutual assistance could be used in German proceedings, provided rule-of-law safeguards (necessity, proportionality, judicial control) are met and no manifest circumvention of German constraints is shown. Later case law consolidated this line, emphasizing structured judicial review rather than categorical exclusion (Korte, 2025). For practitioners, the takeaway is twofold: obtain clear MLA/EIO documentation of the foreign legal basis and maintain audit-ready proportionality logs to withstand admissibility challenges in a legality-sensitive forum like Germany (Bundesverfassungsgericht, 2023).

1. Section 202a of the German Criminal Code (StGB) criminalizes unauthorized access to data that is specially protected against unauthorized access, including data stored or transmitted electronically, magnetically, or otherwise in a manner not immediately perceptible. The offense is punishable by imprisonment for up to three years or a fine (Germany, 2020a).
2. The Act on International Mutual Assistance in Criminal Matters (IRG) governs Germany's procedures for providing and requesting international legal assistance in criminal matters, including the collection and transfer of evidence across borders, the execution of foreign requests, and cooperation with foreign authorities in investigations and prosecutions (Germany, 2020b).

5.2.3. Estonia: Progressive digital legislation and swift cooperation

Estonia's Penal Code (Karistusseadustik) codifies cyber-offences aligned with Budapest and Directive 2013/40/EU (e.g., §§ 206–217 and **§** 216¹ on preparation of computer-related crime), offering full coverage for illegal access/interception, interference, and fraud-type conduct.[1] Estonia has long been an active participant in the Budapest 24/7 Network and an early ratifier of the Convention, reflecting its broader e-governance orientation (European Parliament & Council, 2023).

Estonia's experience during the 2007 distributed attacks catalyzed a whole-of-government cyber capability, including a strong CERT (RIA) and routines for rapid evidence preservation and targeted disclosure via established channels (Estonia, 2017). In practice, this translates into fast responses to urgent subscriber attribution asks when grounded in concrete case identifiers and accompanied by judicial authorization where required. The legal and institutional architecture, Penal Code coverage, competent 24/7 POC, and a digitally mature justice stack minimize dual-criminality friction and reduce cycle time on preservation/execution, particularly when **EIOs** are used with complete Annex A forms and clear necessity statements (Estonia, 2024, consolidated English version, Riigi Teataja).

5.2.4. Hungary: Civil-law codification and evolving procedural tools for e-evidence

Hungary places cyber-offences in Act C of 2012, Chapter XLIII: *illicit access to data* (§ 422), *violation of information systems or related data* (combining unauthorized access/system or data interference in § 423), and *circumvention of technical security measures/misuse of devices* (§ 424). These provisions map closely onto Budapest's substantive template (Hungary, 2025, official English version, NJT).

Procedural and dual-criminality features. The Criminal Code's territorial rules underscore that Hungarian criminal law applies to acts abroad by non-nationals when punishable under both Hungarian law and the foreign law, an explicit dual-criminality orientation relevant to outgoing cooperation and active personality jurisdiction. For incoming or outgoing evidence measures within the EU, Hungary uses the EIO; the competent authority and language practice are set out in EJN materials and national transposition, with prosecutors and courts coordinating on intrusive measures. In practice, complete EIOs with precise data selectors (accounts, IPs, time windows) are executed more smoothly; measures that would not be available domestically or that lack dual criminality face delay or refusal (Eurojust & European Judicial Network, 2019). Hungarian procedure has been progressively

1. The Estonian Penal Code (Karistusseadustik) sets out general criminal offences, including computer-related crimes such as unauthorized access, interception, and interference with data or systems. It provides definitions, sanctions, and procedural rules for prosecuting offences, and is regularly consolidated in English for reference by foreign authorities (Estonia, 2017).

updated (e.g., post-2018 reform of criminal procedure), with courts taking a pragmatic approach to foreign-gathered e-evidence where chain-of-custody documentation is present and defense access is secured. That said, dual-criminality screens and measure-availability tests remain salient, particularly for novel remote searches or covert data captures not mirrored in domestic law.

5.2.5. Comparative insights: Mutual recognition and the EU's e-Evidence turn

The comparative analysis of Rwanda, Germany, Estonia, and Hungary demonstrates that while the substantive criminalization of cyber offences is relatively harmonized through the Budapest Convention and subsequent legislative reforms, practical cooperation continues to encounter friction. The EU's mutual recognition principle, operationalized through instruments such as the European Investigation Order (EIO), provides a model for streamlining evidence sharing across jurisdictions. However, its application to electronic evidence has revealed persistent challenges, prompting the European Commission to advance the e-Evidence Regulation. Against this background, three cross-cutting insights emerge:

- **Substantive alignment is not the bottleneck in these four jurisdictions.** Rwanda's 2018 law, now complemented by the Budapest accession and the EU Member States' codes, all cover the core Budapest offences, reducing the likelihood that pure definitional mismatch will derail cooperation (Council of Europe, 2019).
- **Procedural variability and dual-criminality filters still drive delay.** Even under the EIO, execution can be slowed by domestic measure-availability rules and dual-criminality checks (e.g., in Germany for certain intrusive steps), incomplete forms, or privacy/data-protection constraints. The Commission's implementation review documents these frictions and explicitly calls for complementary tools tailored to electronic evidence (Eurojust & Europol, 2019).
- **Direct-to-provider orders are the new center of gravity.** The e-Evidence Regulation (EU) 2023/1543 introduces European Production and Preservation Orders addressed straight to service providers, with short statutory deadlines and emergency windows designed to stop volatile data from disappearing, while embedding review/notification mechanisms to protect fundamental interests and resolve conflicts of laws. For day-to-day practice, subscriber attribution, basic logs, this should materially reduce lead times compared to classical MLA/EIO routes, provided practitioners use the correct order type, certify necessity or proportionality, and anticipate provider objections (Rwanda, 2018).

5.3. Bottom line for investigators and central authorities

The comparative review highlights that while legislative frameworks are broadly converging, the practical success of cross-border evidence requests still depends on how well investigators and central authorities tailor their strategies to each jurisdiction's procedural requirements. The following operational notes synthesize the key takeaways for practitioners:

- **Rwanda.** Practitioners should cite the precise statutory bases, particularly Articles 16 and 17 of the Law No. 68/2018 on the Prevention and Punishment of Cybercrimes, when seeking production or preservation orders. Where Chapter III requires a judicial mandate, requests should be accompanied by supporting court orders. Since Rwanda's accession to the Budapest Convention, urgent preservation should be routed via the 24/7 contact point under Article 35, which significantly accelerates cross-border responsiveness (Council of Europe, 2001).
- **Germany**. Requests must anticipate dual-criminality and measure-availability checks under the Law on International Mutual Assistance in Criminal Matters (IRG) (Germany, 1982). Submissions should include robust proportionality analyses and, where relevant, documentation of the equivalent foreign legal basis. German courts have shown, in the context of the EncroChat investigations, that while scrutiny of foreign-gathered data is rigorous, properly documented and lawfully obtained evidence will generally be admitted (Higher Regional Court of Hamburg (OLG Hamburg), 2021).
- **Estonia.** Estonia's mature digital infrastructure and proactive use of the Budapest Convention's 24/7 contact point facilitate rapid preservation and execution. To avoid delays, requests should ensure that selectors are tightly scoped and thresholds under Estonian criminal procedure are met (Estonia, 2017). The efficiency of Estonia's system is well documented in Eurojust and Europol reports, which note its best practices in electronic evidence cooperation (Eurojust & Europol, 2019).
- **Hungary.** Investigators should anticipate dual-criminality screening and frame requests through the European Investigation Order (EIO), providing precise selectors and clear necessity and proportionality narratives (Hungary, 2012). For direct-to-provider access, authorities should be prepared to pivot towards the EU's forthcoming e-Evidence Regulation as it is phased in, which will streamline requests to service providers across the EU (European Parliament & Council, 2023).

5.4. Comparative review of reform approaches

Across Rwanda, Germany, Estonia, and Hungary, recent legislative and procedural reforms demonstrate a common acknowledgement that traditional mutual legal assistance (MLA) mechanisms are ill-equipped to match the speed, transnational fluidity, and evidentiary volatility characteristic of digital investigations. Comparative assessment indicates the emergence of four principal strategies that are presently shaping procedural innovation in this domain:

- **Flexible dual-criminality models recognizing functional equivalence of offences.** Traditional dual-criminality checks, requiring that a conduct be criminal in both requesting and requested states, remain a significant source of delay. Some jurisdictions, particularly within the EU, are experimenting with functional equivalence models, whereby offences are assessed based on their core characteristics rather than strict statutory wording. For example, Germany, under the IRG, allows courts to consider whether the underlying harm and intent align with domestic offences, rather than requiring perfect statutory mirroring (Germany, 1982). Rwanda's cybercrime law, complemented by Budapest Convention accession, has also opened the door for interpreting dual-criminality flexibly in cross-border requests (Rwanda, 2018).
- **Treaty-based list exemptions for cybercrime.** A growing trend in EU Member States is to adopt pre-defined lists of cybercrime offences that automatically bypass detailed dual-criminality scrutiny. Such exemptions streamline judicial processing and ensure rapid action, especially for urgent investigative measures. Hungary and Estonia both provide mechanisms under which cybercrime categories enumerated in EU instruments or national implementing legislation can be treated as pre-approved for MLA purposes (Estonia, 2003). Rwanda's accession to the Budapest Convention may allow similar list-based simplifications in future bilateral or multilateral cooperation agreements (Council of Europe, 2001).
- **Fast-track mechanisms for volatile digital evidence.** Digital evidence is inherently ephemeral, from cloud-stored logs to self-deleting malware traces. Estonia, with its mature 24/7 contact point, demonstrates that establishing dedicated rapid-response channels, complemented by narrowly scoped requests and clear selectors, substantially reduces execution times (Eurojust & Europol, 2019). Germany has introduced similar procedural guidance under IRG for high-priority electronic evidence, requiring pre-briefing and proportionality assessments to expedite judicial approval.
- **Budapest Convention 2nd Protocol provisions on expedited preservation and disclosure.** The Second Additional Protocol

> to the Budapest Convention (ETS No. 185, CETS 224) explicitly encourages faster preservation and disclosure procedures, including direct-to-provider measures. While EU Member States like Estonia and Germany are already incorporating these protocols into domestic law, Hungary is gradually phasing in direct-to-provider orders under its civil-law framework (European Commission, 2022).

Taken together, these reform approaches illustrate a convergence of policy goals: reducing procedural bottlenecks, increasing cross-border predictability, and ensuring timely access to digital evidence without compromising fundamental rights. For investigators, the key practical takeaway is that understanding both the procedural nuances and the available expedited channels in each jurisdiction is critical to success.

5.5. Proposed legal and policy solutions

The comparative review highlights that while significant progress has been made in aligning cybercrime frameworks, persistent procedural bottlenecks, particularly around dual criminality, slow MLA execution, and gaps in domestic implementation, continue to undermine effective cross-border cooperation. Addressing these challenges requires coordinated action at both treaty and domestic levels, complemented by procedural innovations and targeted capacity building.

5.5.1. Treaty-level reforms

The Budapest Convention remains the cornerstone of international cooperation against cybercrime. Yet its original offence categories and evidentiary mechanisms reflect early-2000s technological realities. Updating the Convention to include new offences such as large-scale ransomware, deepfake-enabled fraud, and cyber-enabled human trafficking would ensure greater harmonization across legal systems (Council of Europe, 2001). Furthermore, the inclusion of flexible interpretation clauses would enable parties to apply functional equivalence approaches to dual criminality, mitigating delays that arise from strict definitional mismatches. The Second Additional Protocol already points in this direction by expanding expedited cooperation and disclosure channels (Council of Europe, 2021).

5.5.2. Domestic law updates

At the domestic level, states should expand their cybercrime offence lists to align with international standards under the Budapest Convention and its Protocols (European Commission, 2018). For example, Rwanda's Law No. 68/2018 covers key offences but would benefit from updates reflecting newer Budapest Protocol categories, including enhanced powers for expedited preservation (Rwanda, 2018). In the EU, Germany and Hungary already integrate cybercrime-specific

provisions into their mutual assistance frameworks, yet inconsistencies in judicial interpretation remain. Issuing judicial guidance or practice directions on interpreting foreign cybercrime provisions would enhance predictability and ensure that prosecutors and judges treat substantively equivalent offences consistently (Federal Ministry of Justice (Germany), 2020).

5.5.3. Procedural innovations

Procedural innovation is essential to match the volatility of digital evidence. First, the creation of permanent 24/7 cyber liaison officers embedded within judicial authorities could complement the existing Budapest 24/7 network, ensuring real-time communication, technical expertise, and reduced processing delays (Eurojust, 2021). Second, adopting reverse dual criminality waivers for urgent evidence preservation would allow states to provisionally secure volatile data before conducting a full dual-criminality review. Estonia already demonstrates the feasibility of fast-tracking urgent preservation requests, while Germany's IRG framework shows how proportionality safeguards can balance efficiency with rights protection (Schomburg & Lagodny, 2020).

5.5.4. Capacity building

Finally, long-term effectiveness depends on strengthening institutional capacity. Targeted training for judges, prosecutors, and MLA officers on applying flexible dual criminality principles in cybercrime contexts is crucial. This includes modules on interpreting functional equivalence of offences, recognizing the evidentiary volatility of digital data, and applying proportionality assessments in transnational contexts (Council of Europe, 2022). International organizations such as the Council of Europe and Eurojust already run specialized programmes, but national-level judicial academies, such as Rwanda's Institute of Legal Practice and Development (ILPD), should embed these modules into continuing professional development (Institute of Legal Practice and Development, 2023).

6. Findings

The comparative analysis of Rwanda, Germany, Estonia, and Hungary reveals that while substantive alignment on cybercrime offences has improved through the Budapest Convention and related EU instruments, procedural challenges persist in operationalizing cross-border cooperation. The dual criminality principle remains both a safeguard for sovereignty and a bottleneck for efficiency. This dual role underscores the central dilemma of balancing legal autonomy with the practical imperatives of timely evidence collection in the digital age.

6.1. Interpreting key findings

First, the study demonstrates that although substantial progress has been made toward definitional harmonisation of core cyber offences, such alignment is not, in itself, sufficient to eliminate delays in international cooperation. Procedural divergences— particularly regarding the availability of investigative measures, proportionality assessments, and requirements for prior judicial authorisation— continue to generate significant friction in the execution of foreign requests. Even among Member States of the European Union, which are formally bound by principles of mutual recognition, dual criminality assessments and domestic constitutional safeguards remain operative. This indicates that legislative approximation has not fully dismantled entrenched structural constraints.

Second, the rapid evolution of emerging technologies further intensifies these difficulties. Offences such as ransomware-as-a-service (RaaS), AI-driven fraud, and identity crimes facilitated through deepfake technologies frequently occupy regulatory grey areas, particularly in jurisdictions where legislative reform has not kept pace with technological innovation. This misalignment increases the likelihood that urgent requests for electronic evidence may fail to satisfy the dual criminality requirement, especially where one state criminalises novel conduct explicitly, while another subsumes it under more general fraud or data protection provisions.

6.2. Comparative and normative implications

The experience of Germany and Estonia suggests that even advanced jurisdictions committed to the Budapest Convention apply dual criminality with varying degrees of flexibility. Germany's rigorous proportionality and legality review, as illustrated by EncroChat jurisprudence, contrasts with Estonia's more expedited approach facilitated by its digitally mature justice system. Rwanda's accession to the Budapest Convention is a positive step, but practical benefits will depend on how flexibly domestic courts interpret equivalence and how effectively procedural reforms, such as 24/7 contact point operations, are institutionalized.

Normatively, these findings support the growing argument for a functional equivalence model in dual criminality assessments. Such a model, already embedded in certain EU frameworks, evaluates the underlying conduct and harm rather than requiring strict definitional identity. This approach preserves the principle's protective rationale while reducing unnecessary delays that undermine justice in cybercrime cases.

6.3. Practical implications for policy and cooperation

For policymakers, the analysis highlights the importance of embedding expedited cooperation mechanisms, such as those introduced by the Second Additional Protocol to the Budapest Convention, into domestic

law and practice. The adoption of direct-to-provider orders and emergency preservation requests represents a pragmatic response to the volatility of digital evidence. Rwanda, in particular, should leverage its recent treaty commitments to operationalize these tools and issue judicial guidance that promotes consistency in dual criminality evaluations.

At the regional level, the EU's e-Evidence Regulation demonstrates a forward-looking strategy for reconciling sovereignty concerns with investigative urgency. While its principles are not globally transferable in full, they offer a blueprint for interregional cooperation frameworks aimed at ensuring both effectiveness and rights protection.

6.4. Limitations and future research

This study is primarily doctrinal and comparative, focusing on legal texts and selected judicial decisions. It does not incorporate empirical data from law enforcement casework, which could further illuminate how dual criminality operates in practice. Future research should explore the impact of fast-track mechanisms on prosecution outcomes and assess whether flexible dual criminality models improve or compromise fundamental rights protections. Additionally, as new threats such as quantum-enabled attacks and generative AI proliferate, continuous evaluation of the adaptability of current frameworks will be essential.

6.5. Synthesis

In sum, the discussion confirms that while dual criminality remains a legitimate and necessary principle in international cooperation, its rigid application is increasingly incompatible with the operational realities of cybercrime enforcement. Flexible models, combined with technological and procedural innovations, offer the most viable path toward reconciling sovereignty with the need for speed in digital investigations. Without such adaptations, the principle risks becoming an obstacle to justice in an era where time-sensitive evidence can determine the success or failure of cross-border cybercrime prosecutions.

7. Conclusion

This article has examined the persistent dilemma of dual criminality in the context of cybercrime, highlighting its impact on the admissibility of electronic evidence and the efficiency of cross-border investigations. While the Budapest Convention and its Second Protocol provide a shared framework, divergences in domestic offence definitions, procedural safeguards, and sovereignty concerns continue to delay cooperation. Rwanda's recent accession illustrates both the opportunities and challenges facing states outside Europe in aligning with this framework.

The analysis demonstrates that achieving a workable balance between state sovereignty and the urgent need for timely digital evidence is central to future reform. For Rwanda, this requires updating its domestic offence lists, issuing judicial guidance on interpreting foreign provisions, and leveraging the 24/7 network for expedited cooperation. For EU Member States such as Germany, Estonia, and Hungary, the emphasis should be on refining proportionality tests, limiting rigid dual-criminality checks, and operationalizing the e-Evidence Regulation to facilitate direct-to-provider access. Internationally, treaty-level reform of the Budapest Convention, expanding offence categories and embedding flexible dual-criminality standards, will be necessary to ensure harmonization.

Ultimately, the way forward lies in combining legal innovation with institutional capacity building**.** Judicial training, permanent cyber liaison officers, and reverse dual-criminality waivers for urgent preservation requests would ensure that sovereignty is safeguarded without paralyzing effective law enforcement. Only through such reforms can states deliver both cyber justice and sustainable cross-border cooperation in the digital era.

Conflict of interest

The author declared no conflicts of interest.

Ethical considerations

The author has completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Data availability

The dataset generated and analyzed during the current study is available from the corresponding author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

Adeniran, A.A.; Adeniran, A.O.; Familusi, O.B. & Adedayo, O. (2024). "The outlook of cybersecurity in African businesses". *Modelling, Analysis and Simulation in Information Systems*. 1(2). https://doi.org/10.22105/masi.v1i2.54.

Bacher, G.; Faludi, G.; Faludi, G.; Keller, A.; Kerpel, D.; Loranger, K.; Molnár, B. & Wellmann, G. (2021). "Electronic evidence in Hungary: A general overview". *Digital Evidence and Electronic Signature Law Review*. 8: 1-15. https://sas-space.sas.ac.uk/5401/1/1954-2771-1-SM.pdf.

Bąkowski, P. (2023). "Electronic evidence in criminal matters". *EPRS, Members' Research Service, Briefing PE 690.522*. September.

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf.

Boister, N. (2021). *An Introduction to Transnational Criminal Law*. 2nd ed. Oxford University Press.

Bundesverfassungsgericht (Federal Constitutional Court). (2023). *Order of 9 May 2023–2 BvR 558/22 (EncroChat)*. May 9. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2023/05/rk20230509_2bvr055822en.html.

Cao, J. (2025). "A case study of extradition: United States v Meng Wanzhou". *International Journal of Law, Education and Technology*. 23: 45-67. https://ijlet.org/wp-content/uploads/2025/01/1.1.2.pdf.

Council of Europe. (2025). *Rwanda becomes a party to the Budapest Convention on Cybercrime.* January 10. https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-a-party-to-the-budapest-convention-on-cybercrime.

----------. (2022). *Second Additional Protocol to the Convention on Cybercrime (CETS No. 224), arts. 4–7*. https://www.coe.int/en/web/cybercrime/second-additional-protocol.

----------. (2021). *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS No. 224)*. https://www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21lhu/content/opening-coecyber2ap.

----------. (2019). *Cybercrime legislation – Hungary: Legal profile (Act C of 2012 §§ 422–424)*. https://rm.coe.int/octocom-legal-profile-hungary/16809e59cc.

----------. (2013). *Mutual Legal Assistance Manual*. Office in Belgrade. https://www.coe.org.rs.

----------. (2001). *Convention on Cybercrime (ETS No. 185, Budapest, 23 November 2001)*. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

Council of the European Union. (2002). "Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA)". *Official Journal of the European Communities*. L 190: 1-20. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002F0584.

Coupland, H. (2020). "Investigating cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them". *University of York Report.* https://www.york.ac.uk/media/law/documents/eventsandnewsdocs.

Data Protection Act 2018 (No. 7 of 2018) (Ireland).

Edelman, N. (2020). "Global perspectives on cybercrime legislation". *Journal of Infrastructure Policy and Development*. 8(10): 6007. https://doi.org/10.24294/jipd.v8i10.6007.

Estonia. (2024). *Penal Code (Karistusseadustik) (consolidated English version)*. https://www.riigiteataja.ee/en/eli/ee/519012023002/consolide.

----------. (2017). *Penal Code (Karistusseadustik): Consolidated text of 10 January 2017*. Riigikogu. RT I 2001, 61, 364 (original); RT I, 31.12.2016, 2 (last amendment). https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/522012015002/consolide.

European Commission. (2024). *Cybercrime. Migration and Home Affairs.* October 31. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en.

----------. (2022). *Implementing the e-Evidence Regulation: Practical guidance (COM (2022) 355 final)*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2022:355:FULL#:~:text=2.

----------. (2018). *Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (COM (2018) 225 final)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018PC0225.

Eurojust. (2021). *Report on Eurojust's Casework on Cybercrime.* https://www.eurojust.europa.eu/publication/report-eurojusts-casework-cybercrime.

Eurojust & Europol. (2019). *Common challenges in combating cybercrime.* June. https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf.

Eurojust & European Judicial Network. (2019, updated regularly). *Joint Note of Eurojust and the European Judicial Network on the practical application of the European Investigation Order*. https://www.eurojust.europa.eu/publication/joint-note-eurojust-and-ejn-practical-application-european-investigation-order.

European Parliament & Council. (2023). *Regulation (EU) 2023/1543 of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191*. https://eur-lex.europa.eu/eli/reg/2023/1543/oj.

----------. (2014). *Directive 2014/41/EU regarding the European Investigation Order in criminal matters (consolidated version).* [2014] OJ L130/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A02014L0041-20220313.

Federal Ministry of Justice (Germany). (2020). *Guidelines on International Mutual Legal Assistance in Cybercrime.* Berlin. https://www.google.com/url?sa=i&source=web&rct=j&url=https://rm.coe.int/internationalcoop-annex-to-cw-germany/16809f499a&ved=2ahUKEwip2ZLZrseTAxX98LsIHbenHJkQy_kOegYIAQgDEAE&opi=89978449&cd&psig=AOvVaw2i5w-uMewsxPUjMKlrNhPg&ust=1774951220428000.

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. 3rd ed. ITU.

Germany. (2020a). *Act on International Mutual Assistance in Criminal Matters (IRG) (official English translation).* https://www.gesetze-im-internet.de/englisch_irg/englisch_irg.html.

----------. (2020b). *Strafgesetzbuch (StGB) § 202a – Data espionage (official English translation).* https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p0755.

----------. (1982). *Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) [Law on International Mutual Assistance in Criminal Matters], BGBl. I 1982, 2071, as amended*. https://www.gesetze-im-internet.de/irg/BJNR020710982.html.

Habib Zadeh Khiyaban, S. & Sabbar, S. (2022). "Artificial intelligence in credit risk assessment". *Socio-Spatial Studies*. 6(2): 1-14. https://doi.org/10.22034/soc.2022.230178.

Higher Regional Court of Hamburg (OLG Hamburg). (2021, January 29). *EncroChat decision, 2 Ws 93/21*. https://www.landesrecht-hamburg.de/bsha/document/NJRE001454728.

Hungarian Ministry of Justice. (2021). *Amendments to the Criminal Code implementing the Budapest Convention. Budapest*.

Hungary. (2025). *Act C of 2012 on the Criminal Code (official English version, NJT).* https://njt.hu/jogszabaly/en/2012-100-00-00.

----------. (2012). *Act CLXXX of 2012 on Criminal Cooperation with the Member States of the European Union*.

Institute of Legal Practice and Development (Rwanda). (2023). *Judicial Training Curriculum: Electronic Evidence and Cybercrime.* Kigali.

Juszczak, A. & Sason, E. (2023). "The use of electronic evidence in the European Area of freedom, security, and justice: An introduction to the new EU package on e-evidence". *eucrim*. 2: 182. https://doi.org/10.30709/eucrim-2023-014.

Kao, D.Y.; Hsiao, S.C. & Tso, R. (2019). "Analyzing WannaCry ransomware

considering the weapons and exploits". In *2019 21st International Conference on Advanced Communication Technology (ICACT)*. February. https://doi.org/10.23919/ICACT.2019.8702049.

Kaushik, P.; Garg, V.; Priya, A. & Kant, S. (2024). Financial fraud and manipulation: The malicious use of deepfakes in business. In *Deepfakes and their impact on business* (pp. 173–196). IGI Global. https://doi.org/10.4018/979-8-3693-6890-9.ch008.

Korte, M. (2025). "EncroChat–Final word by the German Constitutional Court". *eucrim*. July 15. https://eucrim.eu/news/encrochat-final-word-by-the-german-constitutional-court/.

Kulesza, J. (2019a). *Cybercrime and International Law*. Routledge.

----------. (2019b). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Routledge.

Kurshan, E.; Mehta, D.; Balch, T. & Byrd, D. (2025). "AI-driven fraud, financial and cybercrime: Emerging threats and the evolving landscape of AI versus AI". *International Journal of Semantic Computing*. https://www.researchgate.net/publication/393752134.

Milanovic, M. & Schmiit, M.N. (2020). "Cyber attacks and cyber (mis)information operations during a pandemic". *Journal of National Security Law & Policy*. 11: 247-300. https://doi.org/10.2139/ssrn.3612019.

Plachta, M. (1989). "The role of double criminality in international cooperation in penal matters". In N. Jareborg (Ed.). *Double criminality: Studies in International Criminal Law* (pp. 86-111). Iustus Förlag.

R v Baines [2019] UKSC 14.

Ragni, C. (2023). "Digital evidence in international criminal proceedings and human rights challenges". *International Scientific Conference on International, EU, and Comparative Law Issues: Law in the Age of Modern Technologies*. https://doi.org/10.25234/eclic/28255.

Republic of Rwanda. (2017). *Law No 26/2017 of 31/05/2017 Establishing the National Cyber Security Authority and Determining its Mission, Organisation and Functioning. Official Gazette of the Republic of Rwanda*. No. 27, 3 July. https://rwandalii.org/akn/rw/act/law/2017/26/eng@2017-07-03.

Rwanda. (2018). *Law No. 68/2018 on the Prevention and Punishment of Cybercrimes*. Official Gazette No. Special of 24/08/2018.

Rwanda Investigation Bureau. (2020). *Cybercrime statistics during COVID-19 lockdown*. RIB Press Statement. July 28. https://allafrica.com/stories/202007300062.html.

Salehi, K. & Habib Zadeh Khiyaban, S. (2025). "AI and crime prevention in the academic literature: An integrative review of AI applications in crime prevention". *Code, Cognition and Society*. 1(1): 164-177. https://doi.org/10.22034/ccsr.2025.546552.1016.

Schomburg, W. & Lagodny, O. (2020). *Internationaler Rechtshilfeverkehr in Strafsachen*. 3rd ed. C.H. Beck.

Shahghasemi, E. (2016). "Human Rights against Human Rights: Sexism in Human Rights Discourse for Sakineh Mohammadi". *Society*. 53(6): 614-618. October 26. https://doi.org/10.1007/s12115-016-0073-x.

Shahghasemi, E.; Gholami, F. & Alikhani, Z. (2025). "Global patterns of social media use and political sentiment". *Discover Global Society*. 3(1): 36. https://doi.org/10.1007/s44282-025-00171-y.

Sheppard, S.P. (Ed.). (2020). *Evidence and the Common Law: The Limits of Cross-Border Admissibility in Digital Investigations*. Oxford University Press.

Singh, T. (2024). "Cybercrime and international law: Jurisdictional challenges and enforcement mechanisms". *African Journal of Biomedical Research*. 27(3S): 697. https://doi.org/10.53555/AJBR.v27i3S.2101.

Svantesson, D.J.B. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford University Press.

Tikk, E. & Kaska, K. (2010). "Legal cooperation to investigate cyber incidents: Estonian case study and lessons". *NATO Cooperative Cyber Defense Centre of Excellence.* https://www.ccdcoe.org/uploads/2010/07/Legal_Cooperation_to_Investigate_Cyber_Incidents_Estonian_Case_Study-and_Lessons.pdf.

United Nations. (2000). *Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 29 September 2003), art. 16.* https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf .

United Nations General Assembly. (2022). *Immunity of State Officials from Foreign Criminal Jurisdiction (UN Doc A/77/10).* https://legal.un.org/ilc/reports/2022/english/chp6.pdf.

Wu, C.H. (2021). Sovereignty fever: The territorial turn of global cyber order. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht / Heidelberg Journal of International Law*. 81(3): 651-670. https://doi.org/10.17104/0044-2348-2021-3-651.