International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2025 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Cross–Border Enforcement of Cybercrimes: Jurisdictional Challenges in International Law

Gnana Akshitha Lakkireddy[a]

[a]Mahindra University, Hyderabad, India

Received 12 August 2025; Accepted 11 September 2025; Published 15 September 2025

Digital network statelessness makes it difficult to cohabit with a legal system that is still primarily territorially based and state-centred. Cybercrimes are sometimes planned, carried out, and commercialised in multiple jurisdictions at the same time; attribution, jurisdiction, evidence gathering, extradition and due process are all severely hampered. The main jurisdictional concerns of applying cybercrime laws internationally are examined in this article. It outlines the current treaty framework (with particular emphasis on the Convention on Cybercrime of the Council of Europe, its Second Additional Protocol and mutual legal assistance agreements[1]); theories of prescriptive, enforcement and adjudicative jurisdiction; conflict of laws about compelled disclosure and data protection (particularly data localisation and extraterritorial laws such as the U.S. CLOUD Act[2]); and the tensions caused by divergent substantive definitions od cybercrime. The paper considers practical challenges, such as arbitrary digital evidence, chain-of-custody in various jurisdictions, and sovereignty concerns about remote searches, while recalling case law and state practices. It then outlines several reforms, including harmonising substantive offences and procedural authority, streamlining, right-protective transborder data requests, establishing clearer principles on effects and targeting in cyberspace, establishing human rights-based safeguards for

[1] Second Additional Protocol to the Convention on Cybercrime on Enhance Co-operation and Disclosure of Electronic Evidence CETS No 224/2022 (not yet enforced)
[2] Clarifying Lawful Overseas Use of Data Act 2018

accelerated cooperation, and strengthening technical standards for the authenticity and integrity of electronic evidence. In a networked society, the goal is to strike an operational balance between the right to privacy, expression and a fair trial and effective enforcement.

Keywords*: cybercrime, jurisdiction, mutual legal assistance, Budapest Convention.*

INTRODUCTION

Through the creation of a global, borderless internet that connects people and institutions all over the world, the cyber era has revolutionised communication, trade, and governance. However, when crime is conducted online, this lack of borders causes serious issues. Ransomware assaults, identity theft, phishing scams, and the disruption of vital infrastructure are examples of cybercrimes that are frequently planned in one nation, executed using servers from another, and have the most direct effects on victims in a third nation. Older theories of legal structure, which are deeply embedded in the concepts of territorial sovereignty and state–centric jurisdiction, are becoming less and less acceptable due to this global character.

Although territoriality, nationality and the protective principle are among the jurisdictional bases recognised by international law, their application in cyberspace is far from straightforward. When digital evidence is dispersed over numerous states, it might be difficult to determine where a cybercrime was committed, who committed it, and who is responsible.

Furthermore, state sovereignty precludes unilateral enforcement actions outside of national borders, necessitating the use of avenues such as MLATs. Unfortunately, these systems are frequently too cumbersome and slow to adequately respond to quickly changing cyberthreats or safeguard transient electronic evidence.

Conflicting national laws, data protection regimes, and political interests then exacerbate the ensuing enforcement deficit. These kinds of issues arise when a country's legal requirement for data access clashes with the privacy protections or data localisation requirements of another country. Service providers, many of whom have international operations, are torn between conflicting commitments. Effective investigations are hampered by this legal fragmentation, which therefore runs the risk of weakening protections for human rights, especially the right to privacy, free speech and due process.

The jurisdictional issues in the cross-border enforcement of cybercrimes are severely examined in this essay. It looks at how much state practice and international law attempt to address this conflict between national sovereignty and the worldwide scope of cyber threats. Additionally, it evaluates the function of instruments like the Budapest Convention of Cybercrime, new frameworks like the CLOUD Act,[3] and the ongoing debate over transitional data access. The paper attempts to aid in the development of a more logical, rights-based framework for global collaboration against cybercrime by analysing these issues and proposing workable solutions.

THE INTERNATIONAL LEGAL ARCHITECTURE

The Budapest Convention and Its Protocols: The most well-recognised stand-alone cybercrimes treaty accessible to non-European countries is still the Council of Europe's Convention on Cybercrimes 2001,[4] also known as the Budapest Convention. It includes a mutual legal assistance (MLA) regime specific to electronic evidence, aligns basic offenses (such as unauthorised access, data interference, system interference, device abuse and computer-related fraud), and establishes procedural tools (such as production orders, search and seizure of stored data, real-time traffic data extraction, interception of content, and expedited preservation of stored data). Its second Additional Protocol, which was adopted in 2021 and went into effect for ratifying states in 2023-2024, offers fast-lane procedures for cross-border data access, direct cooperation with service providers on subscriber data, and safeguards for the rule of law and fundamental rights. Even from non-parties, Budapest is a model of reference for domestic law.

Mutual Legal Assistance and Extradition Treaties: Traditional MLA treaties continue to serve as the foundation for evidence sharing across borders. However, MLA is too slow for erratic digital evidence. Delays of months can undermine investigations and render IP logs useless. When behaviour is ambiguous or when dual criminality is unclear because of differing definitions of cybercrime, extradition treaties face similar challenges.

Regional and Domestic Innovations: The U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, which authorises cross-border warrants and bilateral executive agreements; EU tools regulating e-evidence initiatives and the European Investigation Order (EIO)[5] are just a

[3] *Ibid*
[4] Convention on Cybercrime ETS No 185/2004
[5] Directive 2014/41/EU of the European Parliament and of the Council [2014] OJ L130/1

few examples of the laws that have extraterritorial jurisdiction for information stored overseas by local service providers or providers with sufficient jurisdiction contacts. Although they have been applied unevenly, regional instruments in Asia, Africa, and Latin America increasingly mirror transgressions of the Budapest type.

Soft Law and Technical Guidance: By influencing best practices in attribution, evidence handling, and state conduct, international soft law – such as the Tallinn Manual[6] on the International Law Applicable to Cyber Operations, which is not a treaty but has significant influence and technical standards such as the ISO/IEC series on digital evidence complements formal instruments.[7]

JURISDICTION IN CYBERSPACE: PRESCRIPTIVE, ENFORCEMENT, ADJUDICATIVE

Prescriptive Jurisdiction: The right of a state to adopt laws or make certain behaviours illegal is known as prescriptive jurisdiction. Conventional bases consist of:

Territoriality: Actions or outcomes that occur on a state's territory. States commonly claim jurisdiction in the online realm when detrimental effects materialise locally (for example, victims reside locally, systems are situated locally, or losses happen locally), even though servers or offenders are located elsewhere.

Nationality (Active Personality): Foreign – perpetrated crimes overseas.

Passive Personality: Crimes committed against foreigners overseas (more controversial, but increasingly accepted for major crimes).

Protective Principle: Offences that pose a threat to a state's vital interests.

Universality: Saved for a select group of transnational offences (genocide, piracy). Although some advocate limited universal jurisdiction for certain crimes (such as attacks on vital

[6] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017)
[7] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN Doc A/70/174, 2015)

infrastructure) due to their cross-border nature, cybercrime in and of itself is typically not subject to universality.

In practice, multiple states frequently have prescriptive jurisdiction over a single cyber incident, which can cause overlap and even conflict.

Enforcement Jurisdiction: The authority to conduct investigations and exert pressure, whether on or outside of a territory, is known as enforcement jurisdiction. Sovereignty moderated the Lotus principle,[8] which states that states can act only if international law is prohibited. States cannot impose laws in another state without authorisation. This ban covers the following in cyberspace:

Remote searches and transborder access. If done without permission or a valid reason, like an MLA treaty or the Budapest Protocol, retrieving data held on foreign servers, even passively accessed through cloud services, can violate the sovereignty of another state.

It compelled service providers to assist. Although subpoenas issued to domestically incorporated or operating providers may be legitimate locally, their executives may violate foreign data protection laws or blocking regulations.

Adjudicative Jurisdiction: Courts must have jurisdiction over the person or issue. Personal jurisdiction over individuals can be obtained through extradition, arrest or presence. Over corporations, whether a provider targets or conducts substantial business within the forum is determined by minimum contacts or comparable measures (for the jurisdiction). These criteria are challenging in cyberspace since services are available globally without physical locations.

SOURCES OF FRICTION: DIVERGENT LAWS AND CONFLICTING OBLIGATIONS

Privacy and Data Protection: Extensive data protection regulations (such as the EU's GDPR[9]), which limit the release of personal information in the absence of a valid reason and sufficient safeguards, can provide obstacles for investigators. Providers may insist on a formal MLA request or designated treaty channels even in cases where release is feasible. On the other hand, generous warrants may be authorised by the domestic criminal procedure of the country

[8] *France v Turke* [1935] 2 Hudson, World Ct Rep 20
[9] Directive (EU) 2016/680 of the European Parliament and of the Council [2016] OJ L119/89

making the request. The outcome is a choice between disclosing and breaking the privacy laws of the host state or keeping it a secret and facing domestic disdain.

Data Localisation and Sovereignty Assertions: Certain nations restrict cross-border transfers unless regulators give their approval and mandate the domestic storage of particular data categories (such as financial, telecom or vital data). Localisation facilities local access but hinder cross-border services models and foreign probes. Investigators still require forensics that can cross many legal regimes when attackers pass through local infrastructure.

Extraterritorial Compulsion Statutes: Subject to comity studies and executive-level agreements with partner governments, laws such as the CLOUD Act enable domestic courts to order providers under their jurisdiction to release data kept elsewhere. Other jurisdictions have similar tendencies. These rules can lessen the need for MLA, but they run the risk of starting law wars if they conflict with laws that prohibit access or fundamental rights in the area where the data is located.

Dual Criminality and Substantive Divergences: Double criminality is a need for effective collaboration; the action must be illegal in both nations. States, however, use varied approaches to defining cybercrime (e.g., threshold intent for illegal access; breadth of misuse of equipment; criminality of malware possession; consequences of doxxing or deepfakes). Such discrepancies may derail evidence exchange or extradition.

Safe Havens and Non-Cooperation: MLA may struggle in areas with weak political ties; actors operating from non-cooperating nations or regions that are not effectively under government authority may find safe havens. Although they are not extremely strong, encryption, privacy-enhancing technology, and cryptocurrency mixers make asset recovery and attribution even more challenging.

ELECTRONIC EVIDENCE: SPEED, INTEGRITY AND ADMISSIBILITY

Ephemeral Data and the Need for Speed: DHCP assignments, connection records, and certain cloud artefacts are transient. Key leads may be lost as a result of MLA queue or jurisdictional challenge delays. The purpose of the Budapest Convention's expedited preservation directives was to lock down data until the completion of the final production.

Alongside audit and redress processes, the Second Additional Protocol adds faster routes, like direct cooperation for subscriber data in some circumstances.

Authenticity, Integrity and Chain of Custody: Authenticity issues arise when digital evidence is transferred across borders. How can one verify that a disk image or log file is authentic and unaltered? The following are best practices:

- Cryptographic hashing during acquisition and every transfer.
- Comprehensive logs of forensic acquisition (Who, what tools and versions were used, when, where, and how).
- Verifiable time stamps and standard metadata envelopes (take into account trustworthy time sources).
- Where possible, the use of accredited laboratories and verified forensic instruments.

Remote Searches and 123 Agreements: Certain governments allow extraterritorial searches of data thought to be located abroad when it is impossible to determine the location (for example, by probing a botnet) or when there is cause to think that the data may be accessed from within the forum. Such searches are subject to accusations of unlawful extraterritorial application in the absence of an international convention or agreement. Except in extremely rare cases, the tendency is toward solutions under treaties that permit selective cross-border access with judicial oversight and notification to the target state.

Criteria for Admissibility: Digital evidence is subject to various standards in domestic courts. Sovereignty-defying collecting, breach of privacy, or unreliability might all be grounds for exclusionary rules. Internationally recognised authenticity certifications and standardised evidence checklists can reduce litigation and increase predictability.

CASE LAW AND STATE PRACTICE: SELECTED ILLUSTRATIONS

In the case of United States v Ivanov (S.D.N.Y. 2001)[10], a Russian national who operated from Russia compromised financial institutions in the United States. The court's early approval of

[10] *United States v Ivanov* [2001] 175 F Supp 2d 367 (D Conn)

territorial effects for cybercrimes was based on intentional targeting and effects in the United States.

LICRA v Yahoo! (France, early 2000s): French courts ordered Yahoo! to prevent French users from accessing Nazi memorabilia auctions organised in the United States. The case highlighted conflicts between international free-speech protections and local public order principles, which foreshadowed the current disputes about platform cross-border compliance.

Microsoft Ireland Warrant litigation (2016-2018):[11] Emails stored on an Irish server were the subject of a U.S. warrant. Tensions over extraterritorial compulsion and the location-based approach to data were brought to a peak by the dispute, which was finally avoided by the CLOUD Act.

Lauri Love (U.K. 2018):[12] Citing the statutory forum bar and human rights grounds, the U.K. High Court rejected extradition to the U.S. for alleged incursions of U.S. networks. The ruling demonstrates how fairness concerns about forms and health can take precedence over strong prosecution ties.

Reverse-keyword warrants and Google geofence (many U.S. cases):[13] Courts have had trouble defining the scope and specificity of data requests that could capture data or users from other countries. Compliance may clash with international privacy laws even in cases where the asking court has jurisdiction.

Crypto-related prosecution (Many jurisdictions):[14] Examples of how asset-based jurisdiction (seizing money or servers) supports person-based approaches include ransomware payment cases or exchange operator cases (e.g., founders prosecuted in a state for crimes harming victims worldwide).

Three recurring themes emerge from these cases:

- Courts accept broad effects-based jurisdiction over cybercrimes;

[11] *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp* [2016] 829 F3d 197 (2d Cir); *United States v Microsoft Corp* [2018] 584 U.S. ___
[12] *Lauri Love v Government of the United States of America* [2018] EWHC 172 (Admin)
[13] *United States v Chatrie* [2024] No 22-4489 (4th Cir)
[14] *United States v Vinnik* [2017] N D Cal ; *United States v Sterlingov* [2021] DDC

- Enforcement overseas remains severely limited in the absence of consent and thus relies on cooperation mechanisms.
- Rights–based defences of proportionality, fair trial, and forum suitability successfully restrict extradition and data requests.

NORMATIVE AND PRACTICAL REFORMS

Clarify Targeting and Substantial Effects in Cyberspace: States should codify when online conduct targets a forum: purposeful direction at users or system, localisation cues (language, currency, marketing) and technical routing choices. Similarly, substantial effects should require a meaningful nexus (material harm within the forum; not merely foreseeability). A clearer threshold reduces overbroad assertions and forum shopping.

Harmonise Core Offences and Procedural Powers: Building on Budapest, states should:

- Adopt common definitions for illegal access, interference, and fraud, including a culpability threshold.
- Align procedural powers (expedited preservation, production orders, search and seizure of stored data) with calibrated safeguards for journalistic sources, attorney-client materials, and cross-border sensitive data (e.g., health records).
- Incorporate cyber-specific aggravators (critical infrastructure, large-scale attacks, exploration of disasters or public emergencies).

Harmonisation improves dual criminality and predictable cooperation.

Rights-Protective, Fast Cross-Border Data Access: Expedite lawful access while embedding safeguards:

- Provider-to-authority channels for basic subscriber information across borders, with authentication, scope limits, and audit trails.
- Judicial authorisation and proportionality tests for sensitive data, with preference for targeted selectors over bulk demands.
- Notice and challenge mechanisms for users where feasible, with delayed notice in exigent circumstances subject to ex-post review.

- Comity review, where orders conflict with foreign law, a structured comity analysis (taking account of the data's location, the interests of both states, availability of alternatives, and the severity of the crime) should guide modification or denial.

Manage Conflicts with Data Protection and Localisation Laws: States should negotiate bilateral or multilateral data-sharing frameworks that:

- Define permitted categories of data and offences (e.g., serious crime thresholds).
- Require equivalent privacy protections and independent oversight.
- Provide redress for wrongful disclosures.
- Include non-discrimination and purpose limitation clauses.
- Allow transparency reporting by providers and governments.

For localisation regimes, narrow the scope to genuinely critical sectors, allow trusted-partner access through secure gateways, and enable cross-border preservation orders to prevent evidence loss.

Remote Access with Guardrails: When the location of data is unknown or when immediate risk justifies action (e.g., imminent harm, botnet takedowns), narrowly tailored remote access may be permissible if:

- Authorised by a court upon a high evidentiary threshold.
- Limited to specific accounts or nodes, no fishing expeditions.
- Implemented with minimisation, logging, and post-operation notification to affected states through established channels.
- Subject to International transparency (aggregate reporting) and the ability of foreign authorities to seek remedies in case of abuse.

Strengthen Evidentiary Reliability Across Borders: Adopt cross-recognised digital evidence certificates attesting to collection methods, seals, and hashes. Encourage certification of forensic labs and tools to international standards and maintain interoperable metadata schemes for logs, timestamps, and chain-of-custody records.

Prioritise Capacity Building and Trust: Many bottlenecks are not legal but operational. Investment in:

- 24/7 contact points and trusted-flagger relationships with major platforms.
- Standardised MLA request templates, checklists, and triage portals.
- Joint training and secondments between cyber units and data-protection authorities to balance enforcement with rights.

Human Rights Guardrails: Effective enforcement must coexist with freedom of expression, privacy, and fair trial rights. Reforms should embed:

- Proportionality and necessity as operative standards for data access.
- Independent oversight (judicial or equivalent) for intrusive measures.
- Transparency (public reporting on cross-border data requests).
- Remedies (suppression, damages, or administrative sanctions for unlawful intrusions).
- Special protections for journalists, human-rights defenders, and legal privilege.

THE FUTURE: FRAGMENTATION OR INTEROPERABILITY

These are two opposing routes visible. One is fragmentation, which includes retaliatory blocking laws, unilateral extraterritorial orders, hostile privacy regimes, and data localisation. The other is interoperability, which includes mutual recognition of limited, rights-protective orders, established safeguards, and treaty-based fast channels. The latter is better in terms of legitimacy as well as efficiency: transparent, equitable and redressable cross-border collaboration is likely to be more popular with both citizens and providers.

A practical approach combines bridges to a larger set through modular protocols with plurilateral agreements between like-minded states (with strict protections). Technical solutions that balance speed with restrictions include cryptography logging, fixed-width data retention for a limited period of time, and privacy-protecting disclosure (e.g., encrypted selectors, hashed identifiers).

CONCLUSION

Cybercrime thrives on the boundaries of jurisdiction. Criminals use the speed of networks and the slowness of the legal systems. It is challenging for sovereignty-bound governments with different legal systems to gather timely, convincing evidence and to bring criminal charges against offenders without going too far. Although the current treaty regime offers elements such as standardised offences, production and preservation authorities, and expedited channels of collaboration, implementation varies.

Clearer, more focused, and interoperable reforms, rather than just more authorities, are the most encouraging. These include strict authenticity requirements for electronic evidence, investment in trust and capacity, streamlined, rights-based channels for cross-border data disclosure, harmonised definitions of offences and procedural resources, and express tests for targeting and impact. With these, international law can better adjust to the structure of cyberspace, enabling efficient enforcement across borders without compromising the liberties it is meant to protect.