



Original scientific paper

EXTRATERRITORIAL JURISDICTION AND ELECTRONIC EVIDENCE: A NORMATIVE ASSESSMENT OF NEW DIRECT COOPERATION MECHANISMS WITH SERVICE PROVIDERS

Giola Cami, PhD Candidate

University of Szeged, Faculty of Law and Political Sciences
Szeged, Tisza Lajos krt. 54, 6720 Hungary
cami.giola@stud.u-szeged.hu

Krisztina Karsai, PhD, Full Professor

University of Szeged, Faculty of Law and Political Sciences
Szeged, Tisza Lajos krt. 54, 6720 Hungary
karsai.krisztina@szte.hu

ABSTRACT

Transnational criminality and deterritorialized data challenges traditional territorial borders, as electronic communications, cloud storage, and platform-based services enable evidence to be created in one State, stored in another, and controlled by service providers in a third. While criminal justice traditionally grounds enforcement jurisdiction to territorial sovereignty, communications and information technology advances, a significant share of criminal proceedings now depends on data that is fluid - transnational, and de-linked from a stable geographic location.

As a result, extraterritoriality in criminal procedure can no longer be regarded as exceptional but instead constitutes a structural feature of criminal justice. Investigative powers involving coercive measures - such as data searches, seizures, production and preservation orders, are increasingly exercised in transnational contexts, thereby exposing public authorities and private actors alike to overlap and potentially concurring public functions.

This new reality has been addressed through the adoption of new cooperation instruments, which challenge the traditional territorial constraints of procedural powers. This study employs a normative assessment of extraterritoriality through a two-tiered analytical framework. The first part examines extraterritorial jurisdiction in criminal law enshrined in the current legal doctrine debate concerning sovereignty, extended scope of jurisdictions, and inherent nature of electronic

evidence. The second part assesses how extraterritoriality is configured within two selected frameworks, concurrent to each other: (a) Council of Europe's Budapest Convention on Cybercrime, and its Second Protocol; and (b) European Union's Regulation for the European Production Orders and European Preservation Orders. While both institute investigative powers across territorial borders, they are asymmetric with regard to the powers extended to third parties.

We argue that these cooperation mechanisms reflect a model of limited extraterritorial jurisdiction, where the need for efficient investigative powers is weighed against the normative constraints embedded in territorial sovereignty.

Keywords: *Deterritorialized data, Extraterritoriality, Investigative powers, Sovereignty*

1. INTRODUCTION

We have a problem. Proliferation of communication technologies has impacted institutional functioning, particularly within the field of criminal justice. On a yearly basis trillions of security incidents on networks and daily millions of attacks against computers risk security¹, criminal investigations necessitate cross-border electronic evidence gathering. Yet, associated procedural powers sit uneasy with the classical principle of territoriality, embedded within the sovereignty constraints of international law.

Not only cybercrimes, but as well “conventional” offences now yield digital data stored or controlled across borders through decentralized network infrastructures. As a result, domestic criminal investigations collocate transnational borders, where access to evidence may depend less on the territorial nexus, rather more on the architecture of data storage and service provision. For instance, in 2024 Council of the European Union (hereinafter EU) confirmed that 50% of criminal investigations in the Union are conditioned by data located in another jurisdiction.²

This context has exposed a structural tension between traditional principles of criminal jurisdiction and deterritorialized data.³ Territoriality has traditionally served as founding principle of enforcement jurisdiction, constraining the exercise of coercive powers domestically. Yet digital data does not conform to stable territorial assumptions. Data may be fragmented, constantly flowing across jurisdictions, stored in multiple locations, and/or accessed remotely irrespective of physical lo-

¹ Cybercrime Convention Committee (T-CY), *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY – Final Report of the T-CY Cloud Evidence Group T-CY(2016)5*, 16 September 2016, p. 6.

² Council of the European Union, *Better Access to E-Evidence to Fight Crime*, Available at: [<https://www.consilium.europa.eu/en/policies/e-evidence/>], Accessed 6 May 2026.

³ Daskal, J., *The Un-Territoriality of Data*, Yale Law Journal, Vol. 125, 2015, p. 326; Berman, P. S., *Legal Jurisdiction and the Deterritorialization of Data*, Vanderbilt Law Review, Vol. 71, No. 7, 2018, p. 973.

cation.⁴ As a result, the connection between data location and sovereign authority has become ambiguous. The territorial limitations are embodied in the challenges facing mutual legal assistance (hereinafter MLA), mainly burdensome and lengthy procedures of electronic evidence collection.⁵

To remedy this procedural gridlock, legislators have developed new cooperation mechanisms, bypassing the role of public authorities in validating orders, and institutionalizing direct cooperation with private service providers. The new criminal procedural formula bends the principle of territoriality within the enforcement jurisdiction, raising important legal questions on sovereignty, the permissibility of unilateral cross-border investigative powers, and the relationship between enforcement jurisdiction and territoriality in cyberspace. The logic behind the adjusted mechanisms is to remedy the procedural inefficiencies of traditional cooperation mechanisms by circumventing the “control” function of public authorities. Unorthodox or not, the new mechanism’s existence is conditioned by a functional recalibration of territoriality within enforcement jurisdiction.

The current scholarship has examined the deterritorialized nature of electronic data and the emergence of new cooperation mechanism. However, in a comparative landscape less attention has been devoted to whether these mechanisms do fundamentally reconfigure territorial limits of enforcement jurisdiction or instead reinterpret territoriality within international law.

Against this background, this article assesses whether the newly introduced direct cooperation mechanisms redefine the territorial limits of enforcement jurisdiction or, instead constitute a controlled recalibration of territoriality conforming to state sovereignty. We posit that neither the Council of Europe - comprising the Budapest Convention on Cybercrime (hereinafter: Budapest Convention)⁶ and its Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (hereinafter: Second Protocol)⁷ - nor the EU framework consisting of the EU Regulation on the European Production Orders (hereinafter EPOC) and European Preservation Orders

⁴ Daskal, *op. cit.*, note 3, p. 366.

⁵ The estimated efficient timeframe for obtaining evidence would be approximately ten days, compared with the several months often required under traditional MLA procedures. See European Commission, *E-Evidence – Cross-Border Access to Electronic Evidence*, Available at: [https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en], Accessed 6 May 2026.

⁶ Council of Europe, *Convention on Cybercrime*, adopted 23 November 2001, entered into force 1 July 2004, ETS No. 185, art. 1.

⁷ Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, adopted 12 May 2022, ETS No. 224.

(hereinafter EPOC-PR)⁸ abandon territoriality. Rather, both construct models of limited extraterritoriality in which procedural powers are extended only as far as they remain constrained by procedural safeguards protecting sovereignty and fundamental rights.

By developing this concept of limited extraterritoriality and comparatively assessing how it is operationalized within the two legal frameworks, the article contributes to the broader doctrinal debate on the future of enforcement jurisdiction in criminal procedure.

2. METHODOLOGY

This study employs a normative legal assessment of literature and regulations. The first layer of the analysis focuses on the identification of the current state of art of academic discourse, as we review the relevant academic and institutional publications on the subject matter. The doctrinal legal assessment is further strengthened by examining a dual layer of legal norms governed in Council of Europe (hereinafter CoE) and EU frameworks pertaining procedural powers for the access to electronic evidence, and their relationship with principle of territoriality. The study will inherently constitute components of comparative analysis, where compliance and consistence of rules with the territoriality principle is investigated.

3. THE QUESTION ON EXTRATERRITORIALITY

3.1. The limits of sovereignty in international law

Within the framework of public international law, state sovereignty is linked to two fundamental principles - territoriality and non-interference. Each represents, respectively, the positive and negative dimensions of state authority exercise.

Territoriality, as the predominant principle in criminal jurisdiction⁹, constitutes a fundamental constraint within public international law. State jurisdiction is

⁸ Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118.

⁹ The contemporary understanding of sovereignty is bound to the Peace of Westphalia (1648), regarded as foundational to the development of the modern nation-state system. Earlier theoretical reflections on sovereignty can be identified in the work of Jean Bodin, *Six Livres de la République* (1576), where he conceptualizes supreme authority as residing in a political entity capable of maintaining order and terminating conflict. See Bodin, J., *Six Livres de la République*, 1576; Bennoune, K., *Sovereignty vs Suffering? Re-examining Sovereignty and Human Rights through the Lens of Iraq*, European Journal of International Law, Vol. 13, Issue 1, 2002, pp. 243–262.

broadly understood as the power and authority exercised over subjects within its borders. In this sense, territoriality has long served as the primary basis of criminal jurisdiction, enabling states to enact, adjudicate and enforce their criminal laws within their own territory.¹⁰ Fundamentally, international law and the principles governing state jurisdiction are rooted in sovereignty.¹¹ Read together with the logic of *realpolitik* in the international affairs,¹² the principle serves as a pillar legitimating the exercise of criminal jurisdiction within a state's territorial boundaries.¹³

The principle of non-interference, as established in the *Nicaragua* jurisprudence, has been defined as “the right of every sovereign State to conduct its affairs without outside interference”.¹⁴ Though corollary to sovereignty, the principle is uncertain¹⁵, and yet to be assessed on its implications in the increasing digitalized exchange of data.¹⁶ Coercion, as a condition for establishing unlawful intervention, is regarded as interference in the internal affairs of a state. Whereas the notion of *domaine réservé* has been conceptualized in spatial terms, linked to the physical territory of the State, acts of interference would qualify for intrusions such as trespassing or the use of force against a state's territory or troops.¹⁷

While sovereignty has been regarded as particularly exclusive to criminal justice¹⁸, or as conferring the most extensive form of jurisdiction in international law¹⁹, it has not been upheld in the doctrine as *absolute* for the exercise of state authority.²⁰ On the contrary, in the doctrinal debate addressing the tensions between

¹⁰ Liivoja, R., *The Criminal Jurisdiction of States, Foundations*, Journal for Extreme Legal Positivism, Vol. 7, 2010, p. 29.

¹¹ Klabbers, J., *Clinching the Concept of Sovereignty: Wimbledon Redux*, Austrian Review of International and European Law, Vol. 3, 1998, p. 346.

¹² Cryer, R., *International Criminal Law vs State Sovereignty: Another Round?*, European Journal of International Law, Vol. 16, No. 5, 2006, p. 980.

¹³ Westlake, J., *International Law*, Cambridge University Press, Cambridge, 1904; Beale, J. H., *The Jurisdiction of a Sovereign State*, Harvard Law Review, Vol. 36, 2023, p. 241.

¹⁴ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14, para. 202.

¹⁵ Tsagourias, N., Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace, in: Broeders, D.; van den Berg, B. (eds.), *Governing Cyberspace: Behavior, Power and Diplomacy*, Rowman & Littlefield International, London, 2020, p. 45.

¹⁶ Shurson, J., *Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations*, International and Comparative Law Quarterly, Vol. 74, 2025, p. 681.

¹⁷ Moulin, T., *Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward*, Journal of Conflict & Security Law, Vol. 00, No. 0, 2020, pp. 426–430.

¹⁸ Perkins, R. M., *The Territorial Principle in Criminal Law*, UC Law Journal, Vol. 22, No. 5, 1971, p. 1163.

¹⁹ Dixon, M., *Textbook on International Law*, 6th ed., Oxford University Press, Oxford, 2007, p. 154.

²⁰ Bodley, A., *Weakening the Principle of Sovereignty in International Law: The International Criminal Tribunal for the Former Yugoslavia*, New York University Journal of International Law and Politics, Vol. 31, 1999, p. 419.

sovereignty and international law, there have been efforts to reconceptualize sovereignty, challenging its role as a fundamental ordering mechanism.²¹ In doing so, scholarship has moved away from a monolithic approach to state sovereignty, instead defining it as dynamic and flexible²², and capable of evolving within legal frameworks and international relations.²³

The question on sovereignty has been examined in the jurisprudence of the Permanent Court of International Justice. The 1927 landmark *Lotus* case²⁴ confirms that while the principle of territoriality remains a central organizing principle of jurisdiction, it does not preclude the lawful exercise of extraterritorial powers; rather, international law permits the exercise of extraterritorial jurisdiction in the absence of a prohibitive rule.²⁵ However, it was the earlier *Wimbledon* case²⁶ that first elaborated the limits of sovereignty in the context of treaty obligations. The court held that where states adhere to binding international obligations, their sovereign status is not forfeited; rather, the exercise of sovereignty will be restricted within the constraints arising from international law.

As digitalization continues to levitate human interaction in the digital space, the question about sovereignty limitations persists. It raises the issue of whether access to electronic data, especially when directed at foreign-based service providers, constitutes prohibited interference. We argue that even where investigative measures avoid physical intrusion, they may still implicate sovereignty if they bypass or accelerate procedures that would otherwise engage a state's authority. At the same time, the implications for the principle of non-intervention in cases of transnational data access, although relevant, may not amount to the same level of intrusion as classic territorial violations. Rather, they may be understood as a functional limit triggered when procedural powers implicate a state's control within its sovereign domain.

3.2. The Electronic Evidence Inquiry

There is not a commonly established international definition *per se* of electronic evidence²⁷, as different legal regimes have approached it diversely. Notwithstand-

²¹ Klabbers, *op. cit.*, note 11, p. 346; Slaughter, A.-M., *International Law in a World of Liberal States*, European Journal of International Law, Vol. 6, No. 3, 1995, p. 503.

²² Kelsen, H., *Sovereignty and International Law*, Georgetown Law Journal, Vol. 48, No. 4, 1960.

²³ Cryer, *op. cit.*, note 9.

²⁴ *The Case of the S.S. Lotus (France v Turkey)* (1927) PCIJ Rep Series A No. 10, p. 10.

²⁵ *Ibid.*, p. 45.

²⁶ *The S.S. Wimbledon (UK v Germany)* (1923) PCIJ Rep Series A No. 1.

²⁷ Across the literature and jurisprudential discourse, various terms have been employed to describe the data at issue, most notably electronic evidence, digital evidence, and computer data. While these con-

ing, a prevalent legislative approach across jurisdictions has been to distinguish electronic evidence from traditional forms of evidence²⁸, as a minimum threshold for a common international agreed classification. In literature it has been regarded as information of probative value, any electronic information made on a computer²⁹, any data stored or transmitted using a computer³⁰, or mean of proof in legal proceedings.³¹ In the Budapest Convention, it has been provided with the adoption of computer data as “any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”. The Budapest Convention rather than offering a bold definition, adopts a functional and technology-oriented approach grounded in the notion of “computer data.” Read in conjunction with the Explanatory Report, the definition aligns with ISO concept of data, referring to information as processable by computer systems, noting its inherently digital nature.³² However, the Budapest Convention refrains from a narrow understanding of computer data as constrained to the hardware component only. Instead, it adopts a holistic view: as data processed and exchanged across interconnected systems and networks, thus inherently incorporating internet as a component in the classification of electronic data.³³

In acknowledgement of the diversity of legal regimes governing electronic evidence, CoE has further provided with a set of guiding principles, complementary to the notion of electronic evidence: authenticity (preservation of integrity), audit trail (traceability of handling), compliance with law (procedural legality), confidentiality (protection of sensitive data), and admissibility (technical reliability for judicial use).³⁴ Though not legally binding, these principles are relevant. Especially, the authenticity of such data can be compromised due to its inherent

cepts may differ in their technical scope, for the purposes of this study they are treated as functionally equivalent, referring to electronic evidence as developed within the legal frameworks subject to this study.

²⁸ Schafer, B.; Mason, S., *The Characteristics of Electronic Evidence*, in: Mason, S. (ed.), *Electronic Evidence*, 2017.

²⁹ Lange, M. C. S.; Nimsgger, K. M., *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, American Bar Association, 2009, p. 72.

³⁰ Casey, E., *Digital Evidence and Computer Crime*, 3rd ed., Academic Press, 2011, p. 7.

³¹ Mason, S.; Seng, D. (eds.), *Electronic Evidence and Electronic Signatures*, 5th ed., Institute of Advanced Legal Studies for the SAS Humanities Digital Library, 2021, p. 1.

³² Council of Europe, *Explanatory Report to the Convention on Cybercrime*, ETS No. 185, 2001, para. 25.

³³ *Ibid.*, paras. 23–24.

³⁴ Council of Europe, Directorate General of Human Rights and Rule of Law, *Electronic Evidence Guide: A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory*, 2017.

volatile³⁵, ephemeral nature³⁶, as it remains subject to constant change due to the characteristics of the underlying data infrastructure.³⁷ Volatility is defined as the evidence's defining characteristic³⁸, being constantly prone to alteration, loss, or inaccessibility. Furthermore, as data is processed, transferred, and stored in numerous infrastructures, its location may change fluidly, with a measurable impact on legal integrity and evidentiary reliability. Can investigative powers – strongly limited within conventional principles – serve well to access data which constantly flows across multiple territories?

Such fluidity of data reflects data's deterritorialized nature³⁹, where the traditional correlation between jurisdiction and geographic boundaries configures a broken formula, perhaps? Sovereignty, then, may need to be reflective of such reality: as a legal construct intertwined with investigative powers which extend the principles of territoriality and non-interference.⁴⁰

3.3. The Tripartite Structure of Territorial Jurisdiction

Within international law, territoriality is conventionally structured around a tripartite jurisdictional construct: prescriptive, judicial, and enforcement jurisdiction.⁴¹ At the prescriptive level, States enjoy a broader discretion in extending the reach of their legislative authority beyond national borders.⁴² Particularly where

³⁵ Casey, *op. cit.*, note 30; Mason, S.; Seng, D., *The Foundations of Evidence in Electronic Form*, in: Mason, S.; Seng, D. (eds.), *Electronic Evidence*, University of London Press, 2017, p. 48.

³⁶ Currie, R. J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?*, *Canadian Yearbook of International Law*, Vol. 54, 2016, p. 18.

³⁷ Franssen, V.; Tosza, S., *Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges*, in: Franssen, V.; Tosza, S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2022.

³⁸ Erbežnik, A., *Impact of Digital Evidence Gathering on the Criminal Justice System: A Broader Perspective*, in: Franssen, V.; Tosza, S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2022, p. 20; Lasagni, G., *Admissibility of Digital Evidence*, in: Franssen, V.; Tosza, S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2022, p. 128; Cami, G., *Legal Standards for Cross-Border Access to Electronic Evidence in Criminal Procedure: An Albanian Perspective on International Standards*, *Studia Iuridica Lublinensia*, Vol. 33, No. 5, 2024, p. 19.

³⁹ Daskal, *op. cit.*, note 3.

⁴⁰ Currie, *op. cit.*, note 36.

⁴¹ Liivoja, *op. cit.*, note 10, pp. 25–58; Payer, A., *The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries*, *International Criminal Law Review*, Vol. 23, 2023.

⁴² Criddle, E. J., *Extraterritoriality's Empire: How Self-Determination Limits Extraterritorial Lawmaking*, *American Journal of International Law*, 2024, p. 609.

a sufficient connecting nexus exists, what constitutes territorial or extraterritorial has become “increasingly a matter of appreciation”.⁴³ In the descriptive law, hence, the distinction is (being) deconstructed.⁴⁴ This may be justified, for example, by nationality, protective interests, passive personality, universality, or other accepted bases of jurisdiction.⁴⁵

The territoriality question becomes complex at the procedural or enforcement jurisdiction: whether, and under what conditions, a decision adopted by one State may generate legal effects within the territory of another State? The prevailing principle is that decisions emanating from the exercise of State authority carry binding force exclusively within their territorial boundaries where they stem. Embedded in the principle of sovereignty⁴⁶, international law prohibits States from directly exercising coercive powers abroad.⁴⁷ Therefore, if a decision or judgment of one state is intended to produce legal effects in another state, we enter in the field of recognition and enforcement of foreign judgments or foreign decisions. Where cooperation takes place between public authorities, at both CoE and EU level, multiple cooperation mechanisms have been established across different legal fields, including private international law, family law, and criminal law. Depending on the legal context concerned, such mechanisms may operate through *exequatur* procedures, mutual recognition, reciprocity, MLA, or specialized EU instruments.⁴⁸

The next question concerns the legal context where a judicial decision is directed not toward another public authority, but to private actors. This constitutes a novel element in the contemporary cooperation framework. Formal recognition in the traditional sense is no longer required on a case-by-case basis; instead, the regulatory framework itself predetermines the cross-border legal effects of the order, abolishing the need for a separate recognition assessment by the authorities of the State where the service provider is established or where the data is located. The result is a form of controlled extraterritorial effect, operating alongside a reconstructed notion of “European territoriality”⁴⁹, where the connecting factor is no

⁴³ Crawford, J., *Brownlie's Principles of Public International Law*, 9th ed., Oxford University Press, Oxford, 2019.

⁴⁴ Berman, P. S., *The Globalization of Jurisdiction*, University of Pennsylvania Law Review, Vol. 151, No. 2, 2002.

⁴⁵ Ryngaert, C., *Jurisdiction in International Law*, 2nd ed., Oxford University Press, Oxford, 2015.

⁴⁶ Klabbers, *op. cit.*, note 11.

⁴⁷ Criddle, *op. cit.*, note 42, p. 611.

⁴⁸ Ronsfeld, P., *Mutual Recognition and Mutual Trust*, in: Ambos, K.; Rackow, P. (eds.), *The Cambridge Companion to European Criminal Law*, Cambridge University Press, 2023.

⁴⁹ Marzal, T., *The Territorial Reach of European Union Law: A Private International Law Enquiry into the European Union's Spatial Identity*, *International and Comparative Law Quarterly*, Vol. 73, No. 1, 2024.

longer necessarily the physical location of the data or the company, but the provision of services within EU.

3.4. The (Extra)territorial Jurisdiction

Electronic data is location-independent, in fragments and/or with multiple copies, bound to no specific device or closed network⁵⁰, and deployed across different services, providers and/or locations.⁵¹ This context becomes more relevant and central as the ubiquitous use of cloud computing infrastructure⁵² allows data to be stored, processed, and managed across geographically dispersed servers, often without a fixed or identifiable physical location. Result? Data is mobile⁵³ and unpredictable, blurring the distinction between territorial and extraterritorial jurisdiction.⁵⁴ With considerable domestic investigations requiring cross-border access to evidence⁵⁵, investigative powers face numerous challenges, both from a normative and enforcement perspective with regard to extraterritoriality.⁵⁶ The concern arises that, where data is accessed from foreign territories, potential infringements of state sovereignty may occur.⁵⁷

In the debate addressing the “extra mile” of the territorial principle it has been questioned on whether cyberspace ought to be normatively treated as a distinct domain given its borderless and decentralized architecture.⁵⁸ Another approach, opposing a *res nullius* take on cyberspace conceptualizes it as *res communis* - a shared international space analogous to outer space, precluding territorial sovereignty.⁵⁹ These domains of debate are yet to be matured.

⁵⁰ Daskal, *op. cit.*, note 33, p. 366.

⁵¹ Council of Europe, *Criminal Justice Access to Data in the Cloud: Challenges*, Cybercrime Convention Committee (T-CY), T-CY (2015)10, 26 May 2015, p. 9.

⁵² Mell, P.; Grance, T., *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Special Publication 800-145, 2011.

⁵³ Daskal, *op. cit.*, note 3, p. 366.

⁵⁴ Daskal, *op. cit.*, note 3, p. 373.

⁵⁵ Council of the European Union, *Better Access to E-Evidence to Fight Crime*, Available at: [<https://www.consilium.europa.eu/en/policies/e-evidence>], Accessed 17 April 2026.

⁵⁶ Shurson, *op. cit.*, note 16, p. 683.

⁵⁷ Sieber, U.; Neubert, C.-W., *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, in: Lachenmann, F.; Röder, T. J.; Wolfrum, R.; Max Planck Foundation for International Peace and the Rule of Law (eds.), *Max Planck Yearbook of United Nations Law*, Vol. 20, Brill Nijhoff, 2017.

⁵⁸ Currie, *op. cit.*, note 36, pp. 17–18; Wu, T., *Cyberspace Sovereignty? The Internet and the International System*, *Harvard Journal of Law & Technology*, Vol. 10, No. 3, 1997; Johnson, D. R.; Post, D., *Law and Borders: The Rise of Law in Cyberspace*, *Stanford Law Review*, Vol. 48, 1996, pp. 1378–1379.

⁵⁹ Menthe, D. C., *Jurisdiction in Cyberspace: A Theory of International Spaces*, *Michigan Telecommunications and Technology Law Review*, Vol. 4, 1998, pp. 86–87.

The prevailing trajectory of the debate anchors cyberspace within the principle of territoriality. A proposal includes the hyper-territoriality model, where states extend or reassert jurisdiction *vis-à-vis* extended interpretations of territorial criteria.⁶⁰ It relies on a unilateral act of extended territoriality that may lead to fragmentation. Alternatively, a controlled adoption of a transnational cooperation framework is endorsed, rooted in multi-stakeholder participation and procedural interoperability, swaying from pure territorial criteria, yet not eroding it. The model advocates against strict territorial prerequisites that would render the principle a proxy constraint.⁶¹ Within the spirit, a new bold paradigm is presented – *the fourth investigative jurisdiction* – where the binary territory and nationality are swiped instead by new dual proxies: substantial connection and legitimate interest.⁶²

Acknowledging that territoriality principle erodes efficiency of investigative powers governing acquisition of electronic data, the concept of “extended territoriality” allows states to assert enforcement jurisdiction over data that is substantially connected to their territory, even if physically located elsewhere.⁶³ In essence, the new paradigm builds upon the legal vacuum generated by the “un-territoriality” of data in cyberspace, where it is stored, accessed, and controlled.⁶⁴ The adoption of the investigative jurisdiction does not equal the abandonment of the conventional constraints imposed by international law, but rather their recalibration. The model differentiates between direct and indirect enforcement measures, notably through obligations imposed on service providers.

In this study, the concept of limited extraterritoriality is employed as an analytical framework to assess contemporary cross-border procedural powers. It refers to the controlled extension of enforcement jurisdiction beyond territorial borders through legally prescribed procedural mechanisms that remain constrained by safeguards of legality, proportionality, judicial oversight where appropriate, and the protection of fundamental rights. Unlike unrestricted unilateral extraterritorial enforcement, limited extraterritoriality does not replace territoriality as the organizing principle of criminal procedure. Rather, it reflects a recalibration of territoriality in response to the deterritorialized nature of electronic evidence, while

⁶⁰ de La Chapelle, B.; Fehlinger, P., *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*, Global Commission on Internet Governance, Paper Series No. 28, April 2016, p. 12.

⁶¹ Svantesson, D. J. B., *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, AJIL Unbound*, Vol. 109, 2017, p. 70.

⁶² *Ibid.*; Shurson, *op. cit.*, note 16, p. 676; Ryngaert, C., *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, *German Law Journal*, Vol. 24, 2023.

⁶³ Coughlan, S.; Currie, R. J.; Kindred, H. M.; Scassa, T., *Law Beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization*, Irwin Law, 2014, pp. 35–36.

⁶⁴ Daskal, *op. cit.*, note 3.

preserving state sovereignty as the normative boundary governing the exercise of procedural powers.

4. THE QUEST FOR EXTRATERRITORIAL INVESTIGATIVE POWERS: A SHIFT FROM MUTUAL LEGAL ASSISTANCE TO PRODUCTION ORDERS

4.1. The MLA Gridlock: Constraints on Procedural Efficiency

Accessing evidence in a cross-border context and upholding sovereignty principle in criminal law matters has been governed vis-à-vis the instruments of MLA.⁶⁵ Under this framework, coercive measures are governed between public authorities, originally designed for territorially bounded evidence, where the location of evidence is identifiable and stable. When faced with electronic evidence, several challenges have hampered the “muscle” of the authorities to wield efficient measures.

Namely, the chain custody of letter rogatory from issuance to evidence acquisition commonly may take up to 10 (ten) months due to the length and complexity of the procedures involved.⁶⁶ For volatile data, limitations of the MLA framework become unquestionable, referred to as cumbersome and complex.⁶⁷ This legal gridlock is sharpened even more with mass data⁶⁸, or the cloud computing context, as T-CY Cloud Evidence Group concluded that the loss of a stable territorial nexus, combined fragmented control structures renders the identification of applicable jurisdiction and lawful access mechanisms increasingly complex.⁶⁹

Similarly, the need for timely procedural powers has been voiced by the European Commission, noting that MLA mechanisms developed several decades ago no longer meet the demands of efficiency.⁷⁰ Furthermore, it notes that, as a result, states have resorted to expanding national data acquisition tools through direct

⁶⁵ Council of Europe, *European Convention on Mutual Assistance in Criminal Matters*, adopted 20 April 1959, entered into force 12 June 1962, ETS No. 30.

⁶⁶ European Commission, *Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence*, 17 April 2018, Available at: [https://europa.eu/rapid/press-release_MEMO-18-3345_en.htm], Accessed 23 March 2026.

⁶⁷ Council of Europe Cybercrime Convention Committee (T-CY), *The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, 2014, p. 3; Tosza, S., *Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, *Common Market Law Review*, Vol. 61, 2024, p. 150.

⁶⁸ Ryngaert, *op. cit.*, note 62, p. 540.

⁶⁹ Council of Europe Cybercrime Committee, *op. cit.*, note 51, pp. 10–14.

⁷⁰ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM(2018) 225 final, 17 April 2018.

access, raising concerns regarding legal uncertainty, as well as implications for fundamental rights and procedural safeguards.⁷¹

One form of direct access has been police-to-police cooperation, whereby intelligence is shared to support the commencement of criminal proceedings, although in many jurisdictions such intelligence does not meet the threshold for evidentiary use.⁷² Echoing this view, United Nations deemed the traditional means of international cooperation in cybercrimes as not capable for the handling of electronic evidence.⁷³

These challenges, coined as “the MLAT problem” in the academic discourse, constitute a set of interconnected challenges, involving different actors within the system.⁷⁴ It asserts the limited capacity of traditional MLA mechanisms to obtain electronic evidence efficiently, given delays, procedural complexity, and the mismatch between territorial based cooperation and the transnational nature of data.⁷⁵ The solution to the problem has addressed through direct access with service providers, in pursuit of procedural efficiency.

4.2. In(Direct) Cooperation with Service Providers

While legislative measures supporting extended territoriality have been more readily adopted in the prescriptive domain, enforcement jurisdiction remains entrenched in a conservative approach to sovereignty. Yet, with the acceleration of communications and information technology, criminal investigations are faced with a growing impediment to the effective exercise of procedural powers, as data increasingly disregards territorial boundaries. Such procedural impasse no longer is a *hereditas* confined to a handful of jurisdictions, rather a transnational *res communis*, with zero discriminating policy against geography. Addressing this procedural knot, two selective legislative frameworks⁷⁶ are adopting cooperation

⁷¹ *Ibid.*

⁷² Council of Europe Cybercrime Convention Committee (T-CY), *op. cit.*, note 67, p. 7.

⁷³ United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, p. xi.

⁷⁴ Kent, G., *Sharing Investigation-Specific Data with Law Enforcement: An International Approach*, Stanford Public Law Working Paper, 14 February 2014, pp. 6–9. The approach was later embraced and further developed by Currie, *op. cit.*, note 34.

⁷⁵ Currie, *op. cit.*, note 36.

⁷⁶ While this study is constrained to the analysis of the CoE and EU frameworks, a very important legal instrument in this regard is the CLOUD Act (Clarifying Lawful Overseas Use of Data Act), affecting how countries share data across borders. This U.S. law allows the U.S. and other countries to exchange electronic data for criminal investigations, bypassing the MLA procedure. Though the CLOUD Act mainly affects the U.S. law enforcement, it also influences international agreements and data protec-

mechanisms seeking to remedy traditional instruments embedded in sovereignty protectionist foundations.

4.2.1. Direct Cooperation within a Territoriality Centered Framework

In the early 2000s, the CoE addressed the pressing need for improved international co-operation, and envisaged facilitated MLA in the broadest sense.⁷⁷ The Budapest Convention, *per se*, aside from relaxing the dual criminality requirement⁷⁸, did not fully crystallize such proclaimed flexibility. MLA was confirmed as *a priori* cooperation framework among parties, whilst encouraging it to be exercised at the widest extent possible for the collection of electronic evidence.⁷⁹ Two norms in the Budapest Convention advocate for the case of extraterritoriality with regard to the subscriber data, whilst traffic and content data remain subject to MLA procedures.

Article 18(1)(b) of the Budapest Convention permits the extraterritorial use of production orders by allowing authorities to require service providers offering services within their territory to disclose subscriber information within their possession or control, regardless of the provider's location.⁸⁰ This notion of the provider's possession or control was further elaborated in Guidance Note 10. It argues that article 18 (1)(b) may give production orders extraterritorial effect, provided that the service provider offers services within the territory of the requesting Party, irrespective of its physical location.⁸¹

Possession of data refers to subscriber information in the service provider's physical possession, whereas control refers to remotely stored subscriber information under the service provider's control. In other words, the exercise of such procedural powers is directed at service providers on the basis of territorial reach of their services, rather than their place of establishment. The guidance is not binding and does not create new obligations for the parties.⁸² Accordingly, it has been questioned whether this provision constitutes a genuine exercise of extraterritorial jurisdic-

tion rules around the world. See US Department of Justice; European Commission, *EU-US Negotiations on Access to Electronic Evidence*, 2023; US Congress, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*.

⁷⁷ Council of Europe, *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, ETS No. 189, 28 January 2003, para. 3.

⁷⁸ Council of Europe, *Convention on Cybercrime*, *op. cit.*, note 6, art. 25(5).

⁷⁹ Council of Europe, *Convention on Cybercrime*, *op. cit.*, note 6, art. 25(1).

⁸⁰ Council of Europe, *Convention on Cybercrime*, *op. cit.*, note 6, art. 18(1)(b).

⁸¹ Council of Europe Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention)*, T-CY (2015)16, 1 March 2017, p. 3.

⁸² *Ibid.*, p. 6.

tion. Alternatively, it may be understood as a legal power operating within existing territorial limits, given that it does not impose any obligation of recognition or enforcement beyond the framework of the MLA.⁸³ Even if one accepts that the provision reflects an exercise of extended territoriality, the production order may not still amount to a truly extraterritorial practice, given that subjected providers arguably fall into the territorial jurisdiction of the requesting party.⁸⁴

Article 32, by contrast, regulates direct cross-border access to stored computer data that is either (a) publicly available – open source, or (b) has the lawful and voluntary consent of a person who is allowed to share that data.⁸⁵ Similarly, Guidance Note #3, adopted to facilitate effective use and implementation of Article 32, frames the provision as an exception to the principle of territoriality, allowing unilateral transborder access only under consensual conditions.⁸⁶ The notion of “consent” remains insufficiently defined for the purposes of investigative powers, thereby leaving a potential loophole in the regulatory framework. A critical reading of the Guidance shows that this procedural power does not override MLA as the primary mechanism but rather operates alongside it. Article 32 is therefore not conceptualized as a broad assertion of extraterritorial jurisdiction, instead it is limited to clearly defined situations - publicly available data or access based on lawful and voluntary consent.⁸⁷ In doing so, it preserves sovereignty by avoiding any obligation of recognition or enforcement beyond these limited cases. Article 32 therefore serves merely as a pragmatic accommodation to cross-border data realities rather than a doctrinal shift toward extraterritoriality.

In 2014 CoE concluded that the MLA process is timely inefficient, with prolonged procedure up to 24 (twenty-four) months, and many investigations being abandoned.⁸⁸ Among the recommendations proposed, included a preliminary proposal for the consideration of an Additional Protocol to the Budapest Convention to include the possibility for direct cooperation.⁸⁹ In the consequent year, the Cloud

⁸³ Hörnle, J., *Internet Jurisdiction: Law and Practice*, Oxford University Press, Oxford, 2021, pp. 115–145.

⁸⁴ Ryngaert, *op. cit.*, note 62, p. 545.

⁸⁵ Council of Europe, *Convention on Cybercrime*, *op. cit.*, note 6, art. 32.

⁸⁶ Council of Europe Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #3: Transborder Access to Data (Article 32)*, T-CY (2013)7 E, 3 December 2014.

⁸⁷ However, opposing views were also expressed, notably by Boris Vasiliev on behalf of the Russian Federation. See Mallory, J. C. (mod.); Brengelmann, D.; Mohan, C. R.; Vasiliev, B. A., *Sovereignty, International Cooperation and Cyber Security: A Treaty Dialogue*, in: *CYFY 2013: The India Conference on Cyber Security and Cyber Governance*, Observer Research Foundation and FICCI, 2013.

⁸⁸ Council of Europe Cybercrime Convention Committee (T-CY), *op. cit.*, note 67, p. 123.

⁸⁹ Council of Europe Cybercrime Convention Committee (T-CY), *op. cit.*, note 67, pp. 37–39.

Evidence Group⁹⁰ acknowledged that arisen challenges catalyzed by technological advancement embedded jurisdictional uncertainties⁹¹, even more evident when cloud computing enters the equation.⁹² As a result, the Group proposed the adoption of a new protocol aimed at strengthening international cooperation.⁹³

The Second Protocol supplements the Budapest Convention by providing direct access to service providers through the introduction of more nuanced procedural powers with extraterritorial implications. Specifically, two of its provisions operationalize the recommendations developed over the years by pursuing procedural efficiency while seeking to address safeguard imbalances arising from advancement of technology.⁹⁴

Article 6 provides the normative basis for direct cooperation with service providers for domain name registration services. This mechanism enables public authorities to request information about domain name registrants across various jurisdictions. However, it should not be regarded as a conventional coercive extraterritorial power. The reason lies paragraph 2 of the provision, which stipulates that disclosure remains contingent upon the permissibility of such actions under the domestic law of the state in which the entity is located.⁹⁵ Where cooperation is not forthcoming, the Second Protocol does not provide for unilateral enforcement; instead, it requires that authorities revert to consultation mechanisms or alternative forms of cooperation, thereby constraining the extraterritorial reach of the measure. The provision therefore reflects a hybrid model of cooperation in which direct requests are permitted but remain dependent on voluntary compliance and domestic legal frameworks.

By contrast, Article 7 constitutes a more interventionist framework for extraterritorial procedural powers by allowing authorities to issue binding orders directly to service providers located in another Party for the disclosure of subscriber information. It establishes a form of direct enforcement vis-à-vis private actors,

⁹⁰ The Cloud Evidence Group was established in 2014 as a follow-up to earlier work on transborder access to data, mandated to examine criminal justice access to electronic evidence stored in the cloud and across foreign jurisdictions. See Council of Europe Cybercrime Convention Committee (T-CY), *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY*, T-CY (2014)16, 3 December 2014, p. 21.

⁹¹ Council of Europe Cybercrime Convention Committee (T-CY), *op. cit.*, note 51.

⁹² Cybercrime Convention Committee (T-CY), *op. cit.*, note 1, pp. 7–9.

⁹³ Council of Europe, *op. cit.*, note 77, paras. 10–11.

⁹⁴ Traffic data and content data continue to fall exclusively within traditional MLA channels, subject to higher threshold of judicial and inter-state control. See Giola Cami and Krisztina Karsai, 'International Cooperation Mechanisms in Criminal Justice: Human Rights Implications and Sovereignty Constraints in Cross-Border Access to Electronic Evidence' (2025) 2(2) *Balkans Legal, Economic and Social Studies*, p. 93.

⁹⁵ Council of Europe, *op. cit.*, note 7, art. 6(2).

grounded on a territorial nexus. Nevertheless, this mechanism remains carefully balanced by safeguards intended to preserve state sovereignty, including notification requirements to national authorities⁹⁶, and the possibility of consultation.⁹⁷ The provision further makes clear that, in the event of refusal to comply or failure to respond within the prescribed time frame, the issuing authority must revert to MLA or other cooperative channels. Thus, while Article 7 aims to improve procedural efficiency and accommodate human rights considerations, its extraterritorial dimension does not replace MLA but operates alongside it.

4.2.2. Direct cooperation in a mutual trust-based framework

Within the EU framework, the European Investigation Order⁹⁸ (hereinafter EIO) established the first comprehensive mechanism designed to modernize cross-border evidence gathering. Enshrined in the principle of mutual recognition, it was conceived as a single standardized instrument intended to replace the fragmented MLA framework.⁹⁹ The instrument facilitates judicial cooperation through orders circulating directly between competent authorities and thus remains anchored in a territorially based enforcement logic. However, its procedural chain of custody and dependence on executing-state authorities were considered ill-suited to the speed required for obtaining electronic evidence. The legal response to the bottleneck of cross-border data access in criminal proceedings was therefore consolidated through the adoption of the e-evidence package¹⁰⁰, rather than through the amendment of the EIO.¹⁰¹

This development constituted an important step toward greater procedural efficiency and marked a paradigm shift in EU criminal procedure: from authority-to-authority cooperation to direct cooperation with third parties.¹⁰²

⁹⁶ Council of Europe, *op. cit.*, note 7, art. 7(5)(a).

⁹⁷ Council of Europe, *op. cit.*, note 7, art. 7(5)(b).

⁹⁸ Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters [2014] OJ L130/1.

⁹⁹ Tosza, S., *All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order*, New Journal of European Criminal Law, Vol. 11, No. 2, 2020.

¹⁰⁰ Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118; Directive (EU) 2023/1544 of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings [2023] OJ L191/181.

¹⁰¹ European Commission, *op. cit.*, note 70.

¹⁰² Sachoulidou, A., *Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of "Judicial" Cooperation*, New Journal of European

Architected within the principle of mutual recognition - as enshrined in Article 82 of the Treaty on the Functioning of the European Union (hereinafter TFEU), the Regulation is more intrusive in nature compared to the CoE framework, as it challenges more fiercely the traditional limits of mutual recognition. This “intrusion” materializes through the vesting of private service providers with public functions¹⁰³, thereby institutionalizing binding cooperation between judicial authorities third parties. EPOC and EPOC-PR are empowered to reach directly service providers offering services in the Union, irrespective of the actual location of the data or the provider’s infrastructure.¹⁰⁴

This implies that territorial nexus is conditioned to service providers offering services within the Union, even where the provider itself is established outside the EU or the data is stored abroad. In this regard, the location of the company’s headquarters, servers, or storage infrastructure is not determinative.¹⁰⁵ Instead, the Regulation builds jurisdiction around the provider’s connection to the Union market through the offering of services within one or more Member States, as provisioned in Recitals 26 and 29.

Service Provider’s establishment or legal representative in the Union does not itself create jurisdiction; rather, it serves as a procedural mechanism through which authorities may enforce an EPOC in compliance with Article 7 of the Regulation. Such remedial construct allows EU authorities to address orders to foreign-based service providers catering their services within the Union. In doing so, the Regulation decouples jurisdiction from the physical location of the data, acknowledging that cloud-based services and network infrastructures render territorial nexus impractical.¹⁰⁶ The Regulation, hence, stretches the boundaries of indirect cooperation to a model of quasi-direct enforcement vis-à-vis private actors.

Yet, at the same time, the Regulation does not entirely abandon safeguards linked to sovereignty; instead, it aims to balance procedural efficiency with territorial prerogatives through the notification mechanism, proportionality assessments, grounds for refusal, and fundamental rights protections. Particularly, Article 8(1) conditions the issuance of a production order on traffic and content data¹⁰⁷ with an additional notification obligation to public authority in the jurisdiction, where

Criminal Law, Vol. 15, No. 3, 2024.

¹⁰³ Tosza, *op. cit.*, note 67, p. 156.

¹⁰⁴ Regulation (EU) 2023/1543, *op. cit.*, note 8, recital 21.

¹⁰⁵ Regulation (EU) 2023/1543, *op. cit.*, note 8, recital 21.

¹⁰⁶ For the elaborated clarification regarding the “offering services” criterion for the establishment of jurisdiction see European Commission, *op. cit.*, note 70.

¹⁰⁷ Subscriber data, as stipulated in Article 7, is not constrained by such obligation.

the service provider is located. While the Regulation expands enforcement jurisdiction through direct cooperation with service providers, equally it wards off the framework from amounting to an unrestricted coercive power of unilateral extra-territorial enforcement.

4.3. Proportionality Trade-offs: a Procedural Catch 22

4.3.1. Rethinking Territoriality in Criminal Procedure: Toward a Limited Model of Extended Enforcement Jurisdiction

The growing use of investigative powers to obtain cross-border electronic evidence and persisting concerns about insufficient procedural efficiency¹⁰⁸ compels the recognition that extraterritoriality in criminal procedure can no longer be understood as exceptional, or marginal. The un-territorial nature of data¹⁰⁹, cloud infrastructure and encryption challenge conventional legal frameworks strictly embedded in territoriality. The question is therefore no longer whether procedural powers produce extraterritorial effects, but rather how to develop a normative framework capable of accommodating unorthodox legal solutions without dismantling safeguards rooted in sovereignty.

The newly introduced mechanisms - Budapest Convention and its Second Protocol, and the EU Regulation on EPOC and EPOC-PR seek to address this problem. Neither abandons territoriality but rather recalibrates its scope by accommodating forms of extended territoriality in relation to data. Both mechanisms constitute early efforts to facilitate an incremental shift from strict territorial enforcement toward a new model where enforcement jurisdiction operates through a more flexible form of extended territoriality, subject to procedural safeguards.

Procedural powers pursuant to articles 18(1)(b), 32 of the Budapest Convention and articles 6 and 7 of the Second Protocol institute procedural remedies with a controlled extraterritorial implication. They do not abandon MLA as the foundational cooperation model¹¹⁰ but rather operate in tandem with it as complementary mechanisms. These investigative measures though seeking to render possible the “widest extent possible” for the less sensitive subscription data, may lack the “coercive” component and rather grounded on goodwill and cooperation.¹¹¹ This

¹⁰⁸ United Nations Office on Drugs and Crime, *op. cit.*, note 73.

¹⁰⁹ Daskal, *op. cit.*, note 3.

¹¹⁰ Traffic and content data are subject to MLA procedures. Only subscription data collection may be subjected to bypass mechanism.

¹¹¹ Davies, G.; Kennedy-Mayo, D., *The Promise and Pitfalls of the Second Protocol to the Budapest Convention: Assessing Its Impact on EU and UK Cross-Border Criminal Investigations*, New Journal of European

is due to the lack of a binding obligation for service providers to disclose data, rather the “voluntary disclosure” provision favors providers with a discretionary and less stringent procedural position.

The Second Protocol resorts to MLA procedures as a remedy if the service provider supplies not with the requested data, making the mechanism a quasi-efficient for the purpose it was established. Yet, the core problem of the mechanisms under this framework is the asymmetric data protection safeguards among parties, as criticism has questioned the utilization of given instruments.¹¹² Since the Second Protocol was opened for signature in 2021, it has, at the time of writing, been ratified by only four Parties out of 52 signatories. Parties’ hesitation reflects the concern on adhering to a “mutual trust” framework, where parties differentiate in data protection safeguards, institutional capabilities and uneven democratic standards. The imbalance may lead to fragmented application of procedural powers, whereas its implications may affect fundamental rights and procedural guarantees.

In comparison, the cooperation model introduced in the EU Regulation for EPOC and EPOC-PR employs a relatively liberal choice of extended territoriality. Neither does it discard sovereignty. EPOC and EPOC-PR are enforced through a Regulation¹¹³, a conscious choice aimed at harmonizing the cross-border acquisition of electronic evidence between Member States. A fundamentally different approach¹¹⁴, potentially employing asymmetrically the principle of mutual recognition¹¹⁵ and instead rendering the mutual trust principle as rather “absolute”.¹¹⁶ For the intrusive traffic and content data, the Regulation conditions their production

Criminal Law, Vol. 17, No. 1, 2026.

¹¹² Cami, *op. cit.*, note 38; Access Now, *Comments on the Draft Second Additional Protocol to the Budapest Convention on Cybercrime*, 30 April 2021; European Data Protection Supervisor, *Opinion 1/2022 on the Two Proposals for Council Decisions Authorising Member States to Sign and to Ratify, in the Interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, 20 January 2022; European Digital Rights (EDRi), *Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention*, 30 April 2021.

¹¹³ The so far instruments in EU criminal justice enshrined in Article 82 TFEU have been instituted via Directives.

¹¹⁴ Franssen, V., *The European Commission’s E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?*, *European Law Blog*, 12 October 2018, Available at: [<https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement>], Accessed 9 May 2026.

¹¹⁵ Cami; Karsai, *op. cit.*, note 94.

¹¹⁶ Christakis, T., *From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive*, in: Franssen, V.; Tosza, S. (eds.), *Collecting Digital Evidence*, Cambridge University Press, 2025, p. 174.

to additional safeguards, as they may be requested for limited criminal offences,¹¹⁷ and the Order is to be reviewed by a judge in the issuing state.¹¹⁸

Notwithstanding, the model clearly monopolizes the institute of remedy¹¹⁹ to the issuing state. The structural imbalance has been primarily addressed through the “notification knot”, where the “ground for refusal” are expected to protect data and human rights against potential violations of the Charter of Fundamental Rights of the European Union or abusive practices.¹²⁰

The model clearly constructs the procedural relationship as exclusive between the public authorities and service providers, whereas the subjects whose data has been processed remain striped of mechanisms to contest the legality and necessity of measures within the enforcing state.¹²¹ Whether the notification mechanism will be able to leverage its guarantor role without implicating the effectiveness of the direct cooperation instrument will be tested from August 18, 2026 onwards, as the Regulation takes effect. The main concern regards its central role in contributing to the “privatisation” of functions traditionally exercised by public authorities by transferring core compliance responsibilities to service providers.¹²² Similarly, jurisprudence will assess whether the model constitutes a balanced¹²³, and proportional framework.¹²⁴

In both frameworks, private third parties constitute a core component, as they are empowered to serve as guardians of fundamental rights. The question is to what extent are we prepared to vest third parties with public functions and outsource to them the exercise of judgement when assessing the necessity and proportionality¹²⁵ of such coercive measures? Heading, potentially, to the gradual privatization of criminal justice.¹²⁶

¹¹⁷ Regulation (EU) 2023/1543, *op. cit.*, note 8, recital 40. It stipulates that these data may be required for offences that carry at least a three-year maximum custodial sentence.

¹¹⁸ Regulation (EU) 2023/1543, *op. cit.*, note 8, recital 36.

¹¹⁹ Tosza, *op. cit.*, note 99.

¹²⁰ Christakis, *op. cit.*, note 116, p. 186.

¹²¹ Christakis, *op. cit.*, note 116, p. 203.

¹²² Mitsilegas, V., *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-Evidence*, Maastricht Journal of European and Comparative Law, Vol. 25, No. 3, 2018.

¹²³ Tosza, *op. cit.*, note 67, pp. 148–153.

¹²⁴ Juszczak, A.; Sason, E., *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*, No. 2, 2023.

¹²⁵ Topalnakos, P., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, *Eucrim*, No. 2, 2023, p. 200.

¹²⁶ Mitsilegas, *op. cit.*, note 122, pp. 264–265.

In striking a balanced model of coercive measures, the legitimacy of newly developed mechanisms cannot be assessed exclusively through the lens of enforcement efficiency. Otherwise, sovereignty will be treated as an obstacle, rather than the foundational organizing principle of international law. Deterritorialization of data, hence, may not be excused as a reason to ground unrestricted unilateral extraterritoriality, but rather approached with legal solutions that are compatible with the principles of territoriality and sovereignty.¹²⁷

The divergences between the two models of direct cooperation reveal that in tackling the cumbersome timeframes associated with the MLA, new regulations need to be robust to facilitate expedited collection of data across jurisdictions. Within the model of the fourth proposed investigative jurisdiction¹²⁸, a solution may rest in a limited extraterritoriality model – a flexible legal construct where the matter in question is not constrained as a binary question of legality or illegality, but rather a trade-off discourse to accommodate efficiency conditioned to procedural standards commonly shared among parties. The challenge of this model lies in the selective approach to whether such standards should be harmonized or met at a minimum threshold. Answers may be found in mutual trust-based cooperation, as embedded in EU criminal procedure, where the “free circulation” of decisions¹²⁹ facilitates a more effective access to deterritorialized electronic evidence. This framework is a procedural luxury confined within the political and legal context of the EU, where the commonality of standards is a product of harmonization between member states.

Electronic evidence, however, transcends territorial jurisdictions beyond EU without prejudice, and therefore the regulatory responses designed to address it must cater holistic solutions across asymmetric jurisdictions. As in the informal cooperation so far¹³⁰, we may need to consider bilateral agreements between states, operating alongside broader multilateral instruments, within an adjusted trust framework. Such cooperation would be largely constrained and sized by sufficient compatibility between legal systems, robust institutional capacities, commonly shared procedural safeguards and stable long-term relations between the jurisdictions. In this respect, the selective and adjusted mutual trust may not be presumed as *a priori* but instead is progressively constructed upon evidenced reliability, reciprocity, and credibility.

¹²⁷ Kleijssen, J.; Perri, P., *Cybercrime, Evidence and Territoriality: Issues and Options*, in: Netherlands Yearbook of International Law 2016, Springer, 2017.

¹²⁸ Ryngaert, *op. cit.*, note 62; Shurson, *op. cit.*, note 16.

¹²⁹ Karsai, K., *Division of Competences between Member States and the European Union in Criminal Procedural Law*, XXVII FIDE Congress, 2016.

¹³⁰ United Nations Office on Drugs and Crime, *op. cit.*, note 73.

While instituting a fourth jurisdiction in customary international law is not a foreseeable event¹³¹, the model may be applicable in selective states formalizing the direct mechanisms by means of bilateral agreements extending conventional territoriality constrain. There is not an all-size fit solution, rather a model that may capacitate a proportional solution to the problem. Time bound iterative practices will further support a jurisprudence build up, giving rise to a controlled exercise of enforcement jurisdiction as accommodated in international law.

4.3.2. Policing the dark web: anonymity, encryption, and where extraterritoriality becomes secondary

The discussion on cross-border procedural powers becomes more complex in the context of the dark web. The discussion so far has examined how new legal mechanisms accommodate limited forms of extraterritoriality. The dark web, however, presents a distinct yet complementary dimension of this debate. Rather than raising the question of whether enforcement jurisdiction may legitimately extend across borders, the dark web reveals that, in some cases, the main challenge lies in the practical inability to exercise investigative powers at all. Consequently, this section examines whether the proposed model of limited extraterritoriality remains capable of addressing investigative challenges in environments where anonymity and technological indeterminacy render territorial nexus itself uncertain.

Dark web is defined as a deterritorialized space belonging to no single jurisdiction yet implicating them all. Accounting for a substantial portion of the internet and concealed beneath World Wide Web, dark web is understood as a global network of computers, grounded on user anonymity, cryptographically protected communications, and concealed digital transactions.¹³² It is associated as a secretive place operatable by shadowy users accessing hidden services¹³³, and hotbed to illicit activities from good to hacking services, such as malware and denial-of-service attack (DDoS).¹³⁴ Even in cases where investigative authorities are successful in identifying illicit websites, dark web policing is argued to be nearly impossible due to anonymity and encryption.¹³⁵

¹³¹ Shurson, *op. cit.*, note 16.

¹³² Ghappour, A., *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, Yale Law Journal, Vol. 127, 2017, p. 1077.

¹³³ Bradbury, D., *Unveiling the Dark Web*, Network Security, Vol. 4, 2014, p. 14.

¹³⁴ Choi, K.-S.; Lee, C. S., *In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services and the Underground Justice System*, Journal of Contemporary Criminal Justice, 2023, p. 2.

¹³⁵ Davies, G., *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers*, Journal of Criminal Law, Vol. 84, No. 5, 2020.

Achilles' heel is nested in the disrupted infrastructure of the dark web, where users access hidden networks through specialized software such as Tor offering anonymous browsing. Tor allows the user to create a virtual untraceable server, which neither the SP that route the traffic, nor law-enforcement agencies, nor the developers of the Tor project are able to track the server's location.¹³⁶ Unable to identify the location of a targeted device, authorities may not employ any procedural power as discussed so far to collect evidence.¹³⁷ Public authorities have resorted to ad-hoc policing techniques, such as the use of the Open-Source Intelligence, or interrogation of seized data. Despite results, it has been evidenced as inadequate.¹³⁸

While cryptography¹³⁹ constitute a major investigative barrier for law enforcement¹⁴⁰, authorities pursue out of need hacking techniques to bypass encryption and access data, otherwise inaccessible as it is cloaked in anonymity and secure communications technologies. In the U.S. the hacking-based techniques are provisioned as "network investigative techniques", pursuant to the amended Federal Rule of Criminal Procedure 41.¹⁴¹

In essence, the authorities employ malware software in the target transmuting it into a surveillance device, allowing for access to and extract of data. Yet this leapfrog¹⁴² remedial policing mechanism employed through surveillance procedural power poses a significant jurisdictional risk: because the location of the targeted device is unknown at the moment of deployment¹⁴³, such technique may inevitably cross borders, violating sovereignty of foreign jurisdictions where the computer is located. Though normatively the technique is to be engaged within U.S. jurisdiction, it is estimated that 80% of the dark web computers are located abroad, rendering this procedural power an out-of-country mechanism.¹⁴⁴ Despite limited support for the hacking tools employments¹⁴⁵, it has been countered

¹³⁶ Moore, D.; Rid, T., 'Cryptopolitik and the Darknet', 2016, 58(1), Survival 17.

¹³⁷ Ghappour, *op. cit.*, note 132, p. 1093.

¹³⁸ Davies, *op. cit.*, note 135.

¹³⁹ Diffie, W.; Hellman, M. E., *New Directions in Cryptography*, *IEEE Transactions on Information Theory*, Vol. 22, No. 6, 1976.

¹⁴⁰ European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, *op. cit.*, note 120, pp. 18–21.

¹⁴¹ Ghappour, *op. cit.*, note 132, p. 1080.

¹⁴² Ghappour, *op. cit.*, note 132, p. 1095.

¹⁴³ Katyal, N., *Criminal Law in Cyberspace*, *University of Pennsylvania Law Review*, Vol. 149, No. 4, 2001, pp. 1072–1073.

¹⁴⁴ Ghappour, *op. cit.*, note 132, p. 1081.

¹⁴⁵ Bellovin, S. M.; Blaze, M.; Clark, S.; Landau, S., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, *Northwestern Journal of Technology and Intellectual Property*, Vol. 12, No. 1, 2014.

with strong criticism. Google has expressed its concerns about the implications of network investigative techniques, assessing that such policy may corrode nations' sovereignty.¹⁴⁶

In the UK, the hacking has been defined as "Equipment Interference" based on the Investigatory Powers Act 2016, formalizing the use of hacking techniques within a transparent framework. UK endorses rather a safeguarded coercive tool, tied to requirements for the issuance of an equipment interference warrant, including to be approved by the law enforcement chief and a Judicial Commissioner¹⁴⁷, a British Islands connection should be evidenced¹⁴⁸, and for serious crimes¹⁴⁹.

The EU approach on hacking remains fragmented and dependent on national legal systems. European Parliament Study confirmed that law enforcement agencies the Member States subject to study, have used hacking techniques pursuant to the so-called 'grey area' legal provisions, due to the absence of specific legislative provisions.¹⁵⁰ Some states have domestically authorized forms of "lawful hacking", including the Netherlands, France, and Germany.¹⁵¹ Europol and the European Cybercrime Centre's role in coordinating multinational dark web investigations is central, employing covert infiltration, digital forensics, and coordinated device exploitation.¹⁵²

The incompatibility of territorially tied procedural powers and anonymity in cyberspace has presented investigative authorities with an enforcement dilemma: they must either refrain from intervention and risk fostering a culture of impunity for cybercriminals¹⁵³, or employ intrusive tools.

¹⁴⁶ Ghappour, *op. cit.*, note 132, p. 1082.

¹⁴⁷ *Investigatory Powers Act 2016* (UK), s 106(1)(d).

¹⁴⁸ *Investigatory Powers Act 2016* (UK), s 107.

¹⁴⁹ *Investigatory Powers Act 2016* (UK), s 106(3).

¹⁵⁰ European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, 2017, p. 10.

¹⁵¹ *Ibid.*

¹⁵² European Union Agency for Law Enforcement Cooperation (Europol), *Global Cybercrime Crackdown: Over 373 000 Dark Web Sites Shut Down – Authorities from 23 Countries Participate in the Operation*, Europol, 2026, Available at: [<https://www.europol.europa.eu/media-press/newsroom/news/global-cybercrime-crackdown-over-373-000-dark-web-sites-shut-down>], Accessed 10 May 2026.

¹⁵³ In the absence of a conventional justice court, the dark web has developed its own Court of Arbitrage to settle disputes and handle grievances, with outcomes ranging from financial compensations to true identity exposure. See Choi; Lee, *op. cit.*, note 134.

The dark web may be perceived as belonging to no single jurisdiction—or, equally, to all jurisdictions. Extraterritoriality becomes secondary here, not because territoriality loses legal relevance, but because the territorial nexus itself becomes technologically indeterminate. The dark web therefore confirms the relevance of the proposed model, yet it simultaneously constitutes its outer limits. The challenge in this domain is no longer whether enforcement jurisdiction may legitimately extend beyond territorial borders; but whether territoriality remains a connecting factor where the location of data, devices, or users cannot be determined.

5. CONCLUSIONS

The growing volume of criminal investigations necessitating cross-border electronic evidence reflects that territoriality may not be sufficient to function as an unweaving organizing principle for enforcement jurisdiction. Electronic data is volatile, fragmented, and detached from stable territorial connections, whereas efficiency in criminal investigations is dependent on time. MLA framework struggles to satisfy timeframes required, often regarded as cumbersome and inefficient. Newly proposed cooperation mechanisms disrupt the conventional authority to authority circulation, vesting service providers with a central role in criminal justice. This model, primarily, has rendered extended procedural jurisdiction a central legal concern.

Notwithstanding the necessity for efficient procedural powers, the solution cannot nest in unrestricted unilateral enforcement. Territorial sovereignty remains central to international law. The challenge therefore lies in designing procedural frameworks capable of recalibrating investigative efficiency with sovereignty-tied safeguards. The mechanisms examined in this study reflect adjusted models to strike that balance. Whereas the CoE framework adopts a territorial conscious approach, architecting MLA as the foundational cooperation model, it introduces limited forms of direct cooperation. The EU model, by contrast, advances a more intrusive model grounded in the mutual trust paradigm. Both frameworks reflect a gradual recalibration of territoriality rather than its abandonment.

Ultimately, the debate on cross-border access to electronic evidence is not about whether extraterritorial procedural effects should exist, but under what conditions they may be exercised legitimately. The emphasis will be on the development of procedural safeguards as the foundational layer of mechanisms that can constrain investigative power within a growing deterritorialized digital environment. This study assesses positively the model of limited extraterritoriality, whereby cross-border investigative powers may be stretched only insofar as they remain constrained by procedural safeguards, and proportionality. This model advances as

a two-pillar solution, with multilateral and bilateral agreements between parties who trust each other.

The legitimacy of such a model, however, cannot be built solely on investigative efficiency. Cross-border access to electronic evidence should remain conditioned upon a coherent set of normative safeguards, including a clear legal basis, judicial oversight where appropriate, proportionality, effective notification mechanisms, meaningful remedies, and the protection of fundamental rights. Such safeguards are equally necessary to make sure that the involvement of private service providers does not result in an excessive transfer of core public functions traditionally exercised by judicial authorities. Only within such procedural constraints can limited extraterritoriality remain compatible with territorial sovereignty and the rule of law.

Investigations in the dark web elevate this debate to new heights, as anonymity, encryption, and concealed infrastructures challenge the normative assumptions discussed. The question of extraterritoriality here is downgraded as secondary compared to the fundamental problem of law enforcement reliance on hacking-based investigative powers.

REFERENCES

BOOKS AND ARTICLES

1. Access Now, *Comments on the Draft Second Additional Protocol to the Budapest Convention on Cybercrime*, 30 April 2021
2. Beale, J. H., *The Jurisdiction of a Sovereign State*, Harvard Law Review, Vol. 36, 2023, pp. 241–274
3. Bellovin, S. M.; Blaze, M.; Clark, S.; Landau, S., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, Northwestern Journal of Technology and Intellectual Property, Vol. 12, No. 1, 2014, pp. 1–64
4. Bennouné, K., *Sovereignty vs Suffering? Re-examining Sovereignty and Human Rights through the Lens of Iraq*, European Journal of International Law, Vol. 13, Issue 1, 2002, pp. 243–262
5. Berman, P. S., *Legal Jurisdiction and the Deterritorialization of Data*, Vanderbilt Law Review, Vol. 71, No. 7, 2018, pp. 973–996
6. Berman, P. S., *The Globalization of Jurisdiction*, University of Pennsylvania Law Review, Vol. 151, No. 2, 2002, pp. 311–545
7. Bodin, J., *Six Livres de la République*, 1576
8. Bodley, A., *Weakening the Principle of Sovereignty in International Law: The International Criminal Tribunal for the Former Yugoslavia*, New York University Journal of International Law and Politics, Vol. 31, 1999, pp. 417–471
9. Bradbury, D., *Unveiling the Dark Web*, Network Security, Vol. 4, 2014, pp. 14–18

10. Cami, G., *Legal Standards for Cross-Border Access to Electronic Evidence in Criminal Procedure: An Albanian Perspective on International Standards*, *Studia Iuridica Lublinensia*, Vol. 33, No. 5, 2024, pp. 11–30
11. Cami, G.; Karsai, K., *International Cooperation Mechanisms in Criminal Justice: Human Rights Implications and Sovereignty Constraints in Cross-Border Access to Electronic Evidence*, *Balkans Legal, Economic and Social Studies*, Vol. 2, No. 2, 2025, pp. 93–117
12. Casey, E., *Digital Evidence and Computer Crime*, 3rd ed., Academic Press, 2011
13. Choi, K.-S.; Lee, C. S., *In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services and the Underground Justice System*, *Journal of Contemporary Criminal Justice*, 2023
14. Christakis, T., *From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive*, in: Franssen, V.; Tosza, S. (eds.), *Collecting Digital Evidence*, Cambridge University Press, 2025
15. Coughlan, S.; Currie, R. J.; Kindred, H. M.; Scassa, T., *Law Beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization*, Irwin Law, 2014
16. Crawford, J., *Brownlie's Principles of Public International Law*, 9th ed., Oxford University Press, Oxford, 2019
17. Criddle, E. J., *Extraterritoriality's Empire: How Self-Determination Limits Extraterritorial Lawmaking*, *American Journal of International Law*, 2024
18. Cryer, R., *International Criminal Law vs State Sovereignty: Another Round?*, *European Journal of International Law*, Vol. 16, No. 5, 2006, pp. 979–1000
19. Currie, R. J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the 'Next Frontier'?*, *Canadian Yearbook of International Law*, Vol. 54, 2016, pp. 1–51
20. Daskal, J., *The Un-Territoriality of Data*, *Yale Law Journal*, Vol. 125, 2015, pp. 326–398
21. Davies, G., *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers*, *Journal of Criminal Law*, Vol. 84, No. 5, 2020, pp. 408–428
22. Davies, G.; Kennedy-Mayo, D., *The Promise and Pitfalls of the Second Protocol to the Budapest Convention: Assessing Its Impact on EU and UK Cross-Border Criminal Investigations*, *New Journal of European Criminal Law*, Vol. 17, No. 1, 2026, pp. 101–126
23. de La Chapelle, B.; Fehlinger, P., *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*, *Global Commission on Internet Governance*, Paper Series No. 28, April 2016
24. Diffie, W.; Hellman, M. E., *New Directions in Cryptography*, *IEEE Transactions on Information Theory*, Vol. 22, No. 6, 1976, pp. 644–654
25. Dixon, M., *Textbook on International Law*, 6th ed., Oxford University Press, Oxford, 2007
26. Erbežnik, A., *Impact of Digital Evidence Gathering on the Criminal Justice System: A Broader Perspective*, in: Franssen, V.; Tosza, S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2022
27. European Digital Rights (EDRi), *Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention*, 30 April 2021
28. Franssen, V.; Tosza, S., *Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges*, in:

- Franssen, V.; Tosza, S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2022
29. Ghappour, A., *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, Yale Law Journal, Vol. 127, 2017, pp. 1070–1133
 30. Hörnle, J., *Internet Jurisdiction: Law and Practice*, Oxford University Press, Oxford, 2021
 31. Johnson, D. R.; Post, D., *Law and Borders: The Rise of Law in Cyberspace*, Stanford Law Review, Vol. 48, 1996, pp. 1367–1402
 32. Juszczak, A.; Sason, E., *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, No. 2, 2023
 33. Karsai, K., *Division of Competences between Member States and the European Union in Criminal Procedural Law*, XXVII FIDE Congress, 2016
 34. Kelsen, H., *Sovereignty and International Law*, Georgetown Law Journal, Vol. 48, No. 4, 1960, pp. 627–640
 35. Kent, G., *Sharing Investigation-Specific Data with Law Enforcement: An International Approach*, Stanford Public Law Working Paper, 14 February 2014
 36. Klabbers, J., *Clinching the Concept of Sovereignty: Wimbledon Redux*, Austrian Review of International and European Law, Vol. 3, 1998, pp. 345–371
 37. Kleijssen, J.; Perri, P., *Cybercrime, Evidence and Territoriality: Issues and Options*, in: Netherlands Yearbook of International Law 2016, Springer, 2017
 38. Lange, M. C. S.; Nimsger, K. M., *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, American Bar Association, 2009
 39. Lasagni, G., *Admissibility of Digital Evidence*, in: Franssen, V.; Tosza, S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2022
 40. Liivoja, R., *The Criminal Jurisdiction of States*, Foundations—Journal for Extreme Legal Positivism, Vol. 7, 2010, pp. 25–51
 41. Mallory, J. C. (mod.); Brengelmann, D.; Mohan, C. R.; Vasiliev, B. A., *Sovereignty, International Cooperation and Cyber Security: A Treaty Dialogue*, in: CYFY 2013: The India Conference on Cyber Security and Cyber Governance, Observer Research Foundation and FICCI, 2013
 42. Marzal, T., *The Territorial Reach of European Union Law: A Private International Law Enquiry into the European Union's Spatial Identity*, International and Comparative Law Quarterly, Vol. 73, No. 1, 2024, pp. 29–58
 43. Mason, S.; Seng, D. (eds.), *Electronic Evidence and Electronic Signatures*, 5th ed., Institute of Advanced Legal Studies for the SAS Humanities Digital Library, 2021
 44. Mason, S.; Seng, D., *The Foundations of Evidence in Electronic Form*, in: Mason, S.; Seng, D. (eds.), *Electronic Evidence*, University of London Press, 2017
 45. Mell, P.; Grance, T., *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Special Publication 800-145, 2011
 46. Menthe, D. C., *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, pp. 69–103

47. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14
48. Mitsilegas, V., *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-Evidence*, Maastricht Journal of European and Comparative Law, Vol. 25, No. 3, 2018, pp. 263–271
49. Moulin, T., *Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward*, Journal of Conflict & Security Law, Vol. 00, No. 0, 2020, pp. 1–25
50. Payer, A., *The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries*, International Criminal Law Review, Vol. 23, 2023
51. Perkins, R. M., *The Territorial Principle in Criminal Law*, UC Law Journal, Vol. 22, No. 5, 1971, pp. 1155–1172
52. Ronsfeld, P., *Mutual Recognition and Mutual Trust*, in: Ambos, K.; Rackow, P. (eds.), *The Cambridge Companion to European Criminal Law*, Cambridge University Press, 2023
53. Ryngaert, C., *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, German Law Journal, Vol. 24, 2023, pp. 537–558
54. Ryngaert, C., *Jurisdiction in International Law*, 2nd ed., Oxford University Press, Oxford, 2015
55. Sachoulidou, A., *Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of "Judicial" Cooperation*, New Journal of European Criminal Law, Vol. 15, No. 3, 2024, pp. 256–282
56. Schafer, B.; Mason, S., *The Characteristics of Electronic Evidence*, in: Mason, S. (ed.), *Electronic Evidence*, 2017
57. Shurson, J., *Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations*, International and Comparative Law Quarterly, Vol. 74, 2025, pp. 675–702
58. Sieber, U.; Neubert, C.-W., *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, in: Lachenmann, F.; Röder, T. J.; Wolfrum, R.; Max Planck Foundation for International Peace and the Rule of Law (eds.), *Max Planck Yearbook of United Nations Law*, Vol. 20, Brill Nijhoff, 2017
59. Slaughter, A.-M., *International Law in a World of Liberal States*, European Journal of International Law, Vol. 6, No. 3, 1995, pp. 503–538
60. Svantesson, D. J. B., *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft*, AJIL Unbound, Vol. 109, 2017, pp. 69–74
61. Topalnakos, P., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, Eu crim, No. 2, 2023
62. Tosza, S., *All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order*, New Journal of European Criminal Law, Vol. 11, No. 2, 2020
63. Tosza, S., *Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, Common Market Law Review, Vol. 61, 2024, pp. 145–176

64. Tsagourias, N., *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, in: Broeders, D.; van den Berg, B. (eds.), *Governing Cyberspace: Behavior, Power and Diplomacy*, Rowman & Littlefield International, London, 2020, pp. 45–66
65. Westlake, J., *International Law*, Cambridge University Press, Cambridge, 1904
66. Wu, T., *Cyberspace Sovereignty? The Internet and the International System*, *Harvard Journal of Law & Technology*, Vol. 10, No. 3, 1997, pp. 647–666

EU LAW

1. Directive (EU) 2023/1544 of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings [2023] OJ L191/181
2. European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM(2018) 225 final, 17 April 2018
3. European Data Protection Supervisor, Opinion 1/2022 on the Two Proposals for Council Decisions Authorising Member States to Sign and to Ratify, in the Interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, 20 January 2022
4. European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017
5. Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118

CASE LAW

1. Case of *S.S. Lotus* (France v Turkey) (1927) PCIJ Rep. Series A No. 10
2. Case of *S.S. Wimbledon* (UK v Germany) (1923) PCIJ Rep. Series A No. 1

OTHER LEGAL DOCUMENTS

1. Council of Europe Cybercrime Convention Committee (T-CY), *The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, 2014
2. Council of Europe, *Explanatory Report to the Convention on Cybercrime*, ETS No. 185, 2001
3. Council of Europe, Directorate General of Human Rights and Rule of Law, *Electronic Evidence Guide: A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory*, 2017

4. Council of Europe, *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, ETS No. 189, 28 January 2003
5. Council of Europe, *European Convention on Mutual Assistance in Criminal Matters*, adopted 20 April 1959, entered into force 12 June 1962, ETS No. 30
6. Council of Europe, *Criminal Justice Access to Data in the Cloud: Challenges*, Cybercrime Convention Committee (T-CY), T-CY (2015)10, 26 May 2015
7. Council of Europe Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention)*, T-CY (2015)16, 1 March 2017
8. Council of Europe Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #3: Transborder Access to Data (Article 32)*, T-CY (2013)7 E, 3 December 2014
9. Council of Europe Cybercrime Convention Committee (T-CY), *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY*, T-CY (2014)16, 3 December 2014
10. Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, adopted 12 May 2022, ETS No. 224
11. Cybercrime Convention Committee (T-CY), *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY – Final Report of the T-CY Cloud Evidence Group T-CY(2016)5*, 16 September 2016
12. Council of Europe, *Convention on Cybercrime*, adopted 23 November 2001, entered into force 1 July 2004, ETS No. 185
13. Investigatory Powers Act 2016 (UK)
14. United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013
15. US Congress, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*
16. US Department of Justice; European Commission, *EU–US Negotiations on Access to Electronic Evidence*, 2023

WEBSITE REFERENCES

1. Council of the European Union, *Better Access to E-Evidence to Fight Crime*, Available at: [<https://www.consilium.europa.eu/en/policies/e-evidence/>], Accessed 6 May 2026
2. European Commission, *E-Evidence – Cross-Border Access to Electronic Evidence*, Available at: [https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en], Accessed 6 May 2026
3. European Commission, *Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence*, 17 April 2018, Available at: [https://europa.eu/rapid/press-release_MEMO-18-3345_en.htm], Accessed 23 March 2026
4. European Union Agency for Law Enforcement Cooperation (Europol), *Global Cybercrime Crackdown: Over 373 000 Dark Web Sites Shut Down – Authorities from 23 Countries Participate in the Operation*, Europol, 2026, Available at: [<https://www.europol.europa.eu/media-press/newsroom/news/global-cybercrime-crackdown-over-373-000-dark-web-sites-shut-down>], Accessed 10 May 2026