Публично-правовые науки / Public Law Sciences

Научная статья
Original article
DOI: 10.12731/2576-9634-2026-10-3-270
EDN: WKLXIS
UDC 341.24:343.9.018.3

Reconciling cross-border access to stored electronic evidence with sovereignty under the UN Cybercrime Convention

B.S. Aziaka[1], U.I. Nwokorie[2], C.K. Ibiso[3]
[1]Center for International Dispute Settlement, Geneva, Switzerland
[2]Okocha & Okocha Legal Practitioners, Port Harcourt, Nigeria
[3]Babalakin & Co. Legal Practitioners, Port Harcourt, Nigeria

Abstract

Background. This study addresses the tension between efficient cross-border access to stored electronic evidence and state sovereignty, procedural safeguards, and personal-data protection.

Purpose. The objective is to develop and justify a sovereignty-compatible decision sequence under the United Nations Convention against Cybercrime and to identify the limits of Budapest and European Union mechanisms as implementation comparators.

Materials and methods. The study applies doctrinal treaty interpretation under Articles 31 and 32 of the Vienna Convention on the Law of Treaties, functional comparative analysis, and an E/P/N framework across ten categories. Official legal texts and relevant scholarship were reviewed and mapped.

Results. Of the ten categories, preservation is the only E-coded category; eight other categories are P-coded, while the endpoint category comprises three P-coded subfunctions: request response, provider or affected-person remedies, and interstate dispute settlement. Article 40(7) is pivotal because an applicable mutual-assistance treaty ordinarily governs procedure. The proposed sequence separates preservation from disclosure, addresses uncertain data location through Articles 41 and 42, and incorporates the Article 43 traffic-data route.

Conclusions. The Convention supplies the core legal architecture but leaves substantial procedural detail to applicable treaties, reservations, and domestic law; the proposed sequence therefore provides an ex ante implementation framework that preserves sovereign legal functions while maintaining review, proportionality, and data-protection safeguards.

Keywords: cross-border electronic evidence; UN Cybercrime Convention; state sovereignty; stored electronic data; mutual legal assistance; proportionality; personal

data protection; international cooperation; E/P/N Model; functional comparative study; extraterritorial jurisdiction; discretionary powers of the state

For citation. Aziaka, B. S., Nwokorie, U. I., & Ibiso, C. K. (2026). Reconciling cross-border access to stored electronic evidence with sovereignty under the UN Cybercrime Convention. *Russian Studies in Law and Politics*, *10*(3), 4-33. https://doi.org/10.12731/2576-9634-2026-10-3-270

Согласование трансграничного доступа к хранящимся электронным доказательствам с принципом суверенитета в рамках Конвенции ООН о киберпреступности

B.S. Aziaka[1], U.I. Nwokorie[2], C.K. Ibiso[3]
[1]Center for International Dispute Settlement, Женева, Швейцария
[2]Okocha & Okocha Legal Practitioners, Порт-Харкорт, Нигерия
[3]Babalakin & Co. Legal Practitioners, Порт-Харкорт, Нигерия

Аннотация

Обоснование. Настоящее исследование посвящено противоречию между эффективным трансграничным доступом к хранимым электронным доказательствам и государственным суверенитетом, процессуальными гарантиями и защитой персональных данных.

Цель. Цель исследования состоит в разработке и обосновании совместимой с принципом государственного суверенитета последовательности принятия решений в рамках Конвенции Организации Объединенных Наций против киберпреступности, а также в определении пределов применимости механизмов Будапештской конвенции и Европейского союза в качестве сравнительных ориентиров для имплементации.

Материалы и методы. В исследовании применяются доктринальное толкование международных договоров в соответствии со статьями 31 и 32 Венской конвенции о праве международных договоров, функционально-сравнительный анализ и модель E/P/N, охватывающая десять категорий. Были проанализированы и систематизированы официальные правовые тексты и соответствующая научная литература.

Результаты. Из десяти категорий обеспечение сохранности данных является единственной категорией, классифицированной как E; восемь других категорий классифицированы как P, тогда как категория конечных функций включает три подфункции, классифицированные как P: реагирование на запрос, средства правовой защиты поставщика услуг или затронутого лица и урегулирование межгосударственных споров. Статья 40(7) имеет ключевое значение, поскольку применимый

договор о взаимной правовой помощи, как правило, регулирует соответствующую процедуру. Предлагаемая последовательность разграничивает обеспечение сохранности данных и их раскрытие, учитывает неопределенность местонахождения данных посредством механизмов статей 41 и 42 и включает предусмотренный статьей 43 механизм в отношении данных о трафике.

Выводы. Конвенция устанавливает основную правовую архитектуру, однако оставляет существенный объем процессуального регулирования применимым договорам, оговоркам и внутреннему законодательству; поэтому предлагаемая последовательность представляет собой модель имплементации ex ante, обеспечивающую сохранение суверенных правовых функций государства при одновременном сохранении гарантий проверки, пропорциональности и защиты персональных данных.

Ключевые слова: трансграничные электронные доказательства; Конвенция ООН против киберпреступности; государственный суверенитет; хранимые электронные данные; взаимная правовая помощь; пропорциональность; защита персональных данных; международное сотрудничество; модель E/P/N; функционально-сравнительное исследование; экстерриториальная юрисдикция; дискреционные полномочия государства

Для цитирования. Aziaka, B. S., Nwokorie, U. I., & Ibiso, C. K. (2026). Согласование трансграничного доступа к хранящимся электронным доказательствам с принципом суверенитета в рамках Конвенции ООН о киберпреступности. *Russian Studies in Law and Politics / Российские исследования. Право и политика*, *10*(3), 4-33. https://doi.org/10.12731/2576-9634-2026-10-3-270

Introduction

Electronic evidence is now central to many criminal investigations. Yet the authority seeking it and the service provider holding or controlling it are often located in different countries. A European Commission fact sheet accompanying the 2018 e-evidence proposals reported that, at that time, more than half of investigations involved a cross-border request for access to electronic evidence, while electronic evidence was needed in around 85% of criminal investigations and, in two-thirds of those cases, had to be requested from an online service provider in another jurisdiction [11]. Cloud services can also separate the place of the offence, the user, the provider, and the stored data across several jurisdictions [5; 6]. This creates practical pressure because messages, account records, cloud files, and traffic data may be deleted, altered, or moved before a conventional mutual legal assistance request is completed. It also creates legal risk.

Rapid foreign access may bypass courts, privacy rules, or constitutional safeguards in the state connected to the provider or the data. A provider can therefore face a disclosure duty under one legal system and a transfer restriction under another [1; 2]. International assessments continue to identify delay, fragmented procedures, and uneven legal capacity as barriers to lawful access [28]. Too much delay can frustrate an investigation, but poorly controlled access can weaken rights protection and public confidence.

Legal systems have responded in different ways. The Budapest Convention established common offences, procedural powers, expedited preservation, mutual assistance, and a 24/7 cooperation network [7]. Its explanatory materials and Second Additional Protocol later added faster routes for cooperation with service providers, together with procedure-specific and data-protection safeguards [8, 9]. Within the European Union, the framework combines the European Investigation Order, law-enforcement data-protection rules, the GDPR, Directive (EU) 2023/1544, and European Production and Preservation Orders [12-16]. The CLOUD Act takes another route by defining provider duties and allowing executive agreements with qualifying governments [30]. These reforms were intended to speed up preservation and clarify institutional responsibilities. Even so, they allocate different roles to judges, enforcing authorities, providers, and affected persons, so questions about notice, review, refusal, conflicting legal duties, and later use of disclosed data remain contested [2; 6].

The UN Cybercrime Convention brings sovereignty, human rights, data protection, preservation, access, and interstate cooperation into a single global instrument [26; 27]. The United Nations Treaty Collection, rechecked on 7 August 2026, listed 79 signatories and three parties and recorded the Convention as not yet in force [29]. Article 65(1) provides that entry into force occurs on the ninetieth day after deposit of the fortieth instrument of ratification, acceptance, approval, or accession; with only three parties, no calendar date can yet be specified [29]. This interim period is therefore important for preparing implementing legislation, cooperation authorities, domestic procedures, and safeguards before the Convention becomes operational. Because implementation

practice has not yet developed, a close provision-level analysis is timely. In this article, cooperation is treated as sovereignty-compatible when the governing legal route is identified before evidence is sought and when preservation, disclosure, review, use, and refusal safeguards are applied in a transparent order. Put differently, lawful access should preserve the requested state's public functions, applicable procedural guarantees, and international human-rights and data-protection obligations.

Three research questions guide the analysis. RQ1 asks how Articles 3, 5, 6, 22, 24 to 28, 35, 36, 40 to 44, and 63 structure cross-border access to stored electronic evidence while protecting sovereignty and individual rights. RQ2 considers which safeguards in the Budapest and EU electronic-evidence frameworks help clarify matters that the Convention leaves conditional, procedure-specific, or dependent on domestic law. RQ3 asks how those rules can be organised into an ex ante decision framework that distinguishes urgent preservation, expedited traffic-data routing, later access or disclosure, conditional cooperation, refusal, and interstate dispute settlement. The analysis is confined to stored subscriber information, traffic data, and content data relating to offences established under the Convention or to serious crimes within Article 35. When a request combines stored records with prospective traffic collection or content interception, the two components are placed on separate legal tracks because Articles 45 and 46 fall outside this framework.

The objective of this study is to develop and justify a decision-making sequence for cross-border access to stored electronic evidence that ensures compliance with the principle of sovereignty under the United Nations Convention against Cybercrime, as well as to identify the limits of applicability of existing regional mechanisms, particularly the Budapest Convention and EU law.

Literature Review

Cross-border electronic evidence is no longer a narrow issue confined to cybercrime cases; it has become a routine part of criminal procedure. The literature therefore focuses not only on cooperation efficiency but also on lawful authority, evidential reliability, and rights protection [1; 2;

5; 6;28]. Electronic evidence is not a single, uniform category. Different forms of evidence vary in how they are created, stored, authenticated, and used in legal proceedings [21, pp. 51-84].

In this field, sovereignty cannot be reduced to the physical location of a server. It also concerns which state may criminalise conduct, compel a provider, carry out coercive functions, regulate a transfer, and protect the person whose data are requested. Policy standards on government access emphasise legality, legitimate aims, authorisation, proportionality, transparency, limits on later use, and access to remedies [17; 22]. Scholarship on digital sovereignty reaches a similar conclusion: territorial control, infrastructure, regulatory authority, and transnational data governance do not collapse into a single location rule [31; 32]. Scher-Zagier [23] adds a sharper challenge by arguing that the passive-personality basis in Article 22(2)(a) may widen extraterritorial claims against foreigners whose conduct affects a requesting state's nationals. Even when such jurisdiction is lawfully established, Article 5 still prevents one state from exercising public functions reserved to another state's authorities.

Existing regimes approach the problem differently. The Budapest framework combines preservation, production, mutual assistance, provider cooperation, and data-protection safeguards [7-9]. The EU framework is more detailed because it operates within a regional system of mutual recognition and specifies issuing and validating authorities, certificates, deadlines, objections, enforcement procedures, legal representatives, and remedies [11; 12; 15; 16]. Regulation (EU) 2023/1543 entered into force on 17 August 2023 and applies from 18 August 2026. The African Union's Malabo Convention takes a different regional approach. Articles 8 to 19 establish core data-protection rules and oversight arrangements, while Articles 24 to 31 address cybersecurity, cybercrime, harmonisation, and institutional capacity. It does not create a cross-border production-order system comparable to the EU framework [3, Arts. 8-19, 24-31]. The Malabo Convention is therefore used here as contextual evidence rather than as a formal comparator in the classification.

The UN Convention gathers these issues in one text, but its rules are spread across the general, procedural, and cooperation chapters. Recent

analysis describes the Convention as an important cooperation instrument while stressing that its operation will depend heavily on national law and institutional capacity [18]. Other scholarship links the negotiations to competing understandings of territorial and digital sovereignty [24; 31]. Civil-society and industry submissions raise a more critical concern: broad cooperation powers, weak authorisation, secrecy, and uneven domestic safeguards may expose journalists, cybersecurity researchers, civil-society actors, and political opponents to misuse [4; 10; 19]. Articles 5 and 6 matter, but citing them is not enough. The practical strength of review and remedies will also depend on domestic institutions and on whether requested states are willing to examine the purpose and likely consequences of a request.

Taken together, the literature explains the main cooperation mechanisms and the principal rights risks. The targeted search undertaken for this study did not reveal a Convention-specific sequence that first identifies scope and the applicable mutual-assistance route, then separates preservation from access or disclosure, and finally distinguishes correctable defects from lawful grounds for postponement or refusal. This article addresses that narrower operational-integration gap. It does not present the proposed sequence as the only permissible interpretation, and it does not treat textual specificity as proof of effective implementation.

Methodology

This study combines doctrinal treaty interpretation with functional comparative legal analysis, supported by a structured classification of individual provisions. Official legal texts form the core of the corpus. Peer-reviewed scholarship and institutional materials are used to identify competing interpretations and possible implementation risks. The legal materials were drawn from repositories maintained by the United Nations, the Council of Europe, EUR-Lex, the African Union, the OECD, and the United States Congress and were checked on 14 July 2026; the UN Treaty Collection status was rechecked on 7 August 2026. Interpretation followed Article 31 of the Vienna Convention on the Law of Treaties. The analysis began with the ordinary meaning of each provision, read in

good faith, in context, and in light of the Convention's object and purpose. The preamble, definitions, internal cross-references, relationship clauses, reservations, and declarations were treated as part of that context. Article 32 was used as a supplementary interpretive route, available to confirm the Article 31 reading or to address an ambiguity or an unreasonable result, rather than as a basis for displacing clear treaty wording [25]. Comparator rules were used to illuminate implementation choices; they were not treated as sources of additional obligations under the UN Convention. RQ1 was addressed through an integrated reading of the Convention, RQ2 through functional comparison with the Budapest and EU frameworks, and RQ3 through synthesis of the resulting rules into a proposed decision framework.

Secondary literature was identified through targeted searches in Google Scholar, Crossref Metadata Search, SSRN, and major publisher databases, supplemented by reference-list checking. Searches were guided by the research questions and focused on cross-border electronic evidence, mutual legal assistance, jurisdiction, sovereignty, data protection, and provider disclosure. Priority was given to English-language sources published between January 2020 and July 2026, while older primary legal texts and important interpretive authorities were retained where necessary. The search was targeted rather than systematic and was used to support doctrinal analysis, not as a systematic review or bibliometric study; it may therefore have missed relevant work indexed elsewhere or framed in different terms. Primary legal materials remained controlling, while secondary literature was used to identify competing interpretations and implementation concerns across the selected frameworks. This weighting reflects the study's doctrinal rather than empirical design.

Secondary sources were retained only where they directly informed the doctrinal questions concerning stored electronic evidence, cross-border cooperation, jurisdiction, data protection, provider obligations, or remedies. The study excludes intelligence surveillance, military cyber operations, civil discovery, forensic admissibility, and the merits of live interception. Mixed requests are considered only to the extent needed to identify the boundary between stored evidence and the real-time proce-

dures in Articles 45 and 46. The Convention provisions examined most closely are Articles 3, 5, 6, 22, 24 to 28, 35, 36, 40 to 44, and 63.

The Budapest and EU frameworks were chosen because they contain developed procedures for preservation, provider cooperation, production, enforcement, data protection, and remedies that perform the same legal functions as the Convention's stored-evidence rules. The comparison is functional rather than geographically representative. It does not assume that a regional system of mutual recognition and a global treaty rest on equivalent institutional foundations. The Budapest and EU columns are instrument clusters, while the UN column evaluates the design of a single global convention before a body of national implementation practice has developed. The codes therefore compare textual and institutional specificity at the selected level of aggregation; they do not compare complete domestic implementation regimes. Non-European instruments, including the Malabo Convention, were used as contextual checks on the article's global claims but were not classified where they lacked functionally comparable cross-border evidence procedures.

The classification is intended to make the legal comparison transparent, not to produce a quantitative score. The E/P/N scheme is a doctrinal analytical framework for organising and comparing the legal specificity of treaty provisions; it is not an empirical content-coding instrument or a set of statistical variables. Kuckartz and Rädiker [20] informed the use of explicit category definitions, decision rules, and documented reconsideration of ambiguous cases, but the substantive classifications remain reasoned doctrinal legal judgments. Table 1 sets out ten categories and the threshold for assigning E, P, or N. For each category, the elements listed in the operational legal question were treated as its core elements. E was assigned only where the central legal route and all or substantially all core elements were expressly stated without material reliance on domestic law, another treaty, a reservation, or procedure-specific detail. P was assigned where at least one core element remained materially dependent on such external law or was express only for a limited procedure. N was reserved for the absence of a relevant rule. The unit of analysis is the functional category at framework level, supported by provision-level

mapping and full consideration of relevant cross-references. The final category contains three distinct endpoint functions: request response, provider or affected-person remedies, and interstate settlement. To avoid treating them as legally equivalent, Table 2 and Table S1 report separate subcodes for those three functions; N/A is used where interstate settlement falls outside the selected instrument cluster.

Table 1.

Structured Classification Categories and Coding Rules

Category	Operational legal question	E	P or N
Jurisdictional and cooperation nexus	Does the framework identify substantive scope, offence jurisdiction, territorial or provider links, limits on extraterritorial action, and the applicable cooperation route?	The essential nexus and route are expressly stated.	P if the rules are distributed or materially dependent on another treaty or domestic law; N if absent.
Competent authority	Does it identify who may issue, validate, receive, execute, or enforce the request?	The relevant institutional roles are expressly assigned.	P if only some roles are specified or domestic law supplies the main detail; N if absent.
Specificity	Must the request identify the authority, facts, data, period, purpose, and relationship to the offence?	Essential request content is expressly stated.	P if content is general, indirect, or dependent on another instrument; N if absent.
Necessity and time sensitivity	Must the authority establish need, relevance, vulnerability to loss, or grounds for expedited handling?	Operational necessity or urgency requirements are expressly stated.	P if expressed only as a principle or for limited procedures; N if absent.
Proportionality	Must the measure be limited in scope and duration and balanced against protected interests?	An operational proportionality test is stated.	P if proportionality is required but its test is supplied mainly by domestic law; N if absent.

Category	Operational legal question	E	P or N
Independent review	Is judicial or functionally independent control required or available, with an effective remedy?	Independent control and remedy rules are expressly specified.	P if conditional, procedure-specific, or dependent on domestic law; N if absent.
Data protection and use	Are transfer, purpose, use, retention, onward transfer, sensitive data, and remedies controlled?	The essential controls are expressly stated across the category.	P if substantial elements depend on domestic or general law; N if absent.
Preservation	Can specified stored data be secured before access or disclosure is decided?	An express preservation procedure is provided.	P if preservation is indirect or incomplete; N if absent.
Access and disclosure	Does the framework govern search, production, securing, or transfer of stored data?	The access or disclosure route and essential procedure are expressly stated.	P if execution depends materially on another treaty or domestic law; N if absent.
Response, remedies, and interstate dispute handling (separate subcodes)	Does the framework address (a) consultation, conditions, partial compliance, postponement, refusal, and reasons; (b) provider or affected-person review and remedies; and (c) interstate settlement?	A separate E code is assigned to each subfunction when its central route and core procedure are expressly stated.	P if a subfunction is partial, reserved, procedure-specific, or mainly domestic; N if absent; N/A if interstate settlement falls outside the selected instrument cluster.

Note. E indicates that the framework states the relevant rule and the central route together with all or substantially all core elements listed in the operational question. P indicates that at least one core element depends materially on domestic law, an applicable treaty, a reservation, or procedure-specific detail. N indicates that no relevant rule was identified. N/A is used only for the interstate-settlement subcode where that function falls outside the selected instrument cluster. The codes compare textual and institutional specificity, not practical effectiveness or rights protection.

Classification followed three steps. First, the relevant provisions were identified and mapped to one or more functional categories. Second, each category was read in its full legal setting, including cross-references, domestic-law qualifications, reservations, and rules governing the relationship with other treaties. Third, a framework-level code was assigned. E was used only when the provisions assessed stated the central legal route and all or substantially all core elements of the category. P was used when an express rule covered only part of the category or when implementation depended materially on domestic law, an applicable mutual-assistance treaty, a reservation, or a procedure confined to particular requests. N was reserved for cases in which no relevant rule was identified. Where express and dependent elements appeared together, the more cautious P code was retained unless the express provisions covered the category as defined in Table 1. The three endpoint functions were classified separately rather than compressed into a single result.

The classification was conducted as a single-researcher doctrinal analysis. After the initial matrix was completed, it was rechecked provision by provision against the category definitions, cross-references, domestic-law qualifications, reservations, and the relationship between the instruments. Ambiguous entries were reconsidered before the final framework-level code was retained. No statistical inter-rater coefficient was calculated because the exercise evaluates legal interpretation against stated doctrinal criteria rather than estimating agreement between independent empirical coders. Reliability is instead supported by explicit definitions, cautious aggregation, provision-level traceability, and a supplementary matrix that records the principal legal basis for each code. These measures reduce unexplained classification, although they cannot remove selection and interpretive judgment.

In the final stage, the doctrinal and comparative findings were brought together in a proposed decision framework. Treaty requirements were kept separate from comparator-informed implementation guidance, and every step had to be traceable to a Convention provision or clearly marked as a prudential safeguard. Because the Convention had not entered into force and had only three parties on the verification date, the study evaluates legal

design rather than actual performance. The framework will therefore need to be tested against implementing laws, request files, judicial decisions, provider practice, declarations, and reservations after entry into force [29].

Comparative Findings

The comparison produces a clear but qualified result. Relevant provisions were identified in each of the ten preselected categories, but the degree of operational specificity varies. Under the cautious aggregation rule, preservation is the Convention's only E classification. The jurisdictional and cooperation nexus, competent authority, request specificity, necessity and time sensitivity, proportionality, independent review, data protection, and access and disclosure are coded P. The endpoint category is reported through separate subcodes: request response is P, provider or affected-person remedies are P, and interstate dispute settlement is P. These results do not mean that the Convention ignores the P-coded matters. Rather, the relevant rules are spread across several provisions, apply only to particular procedures, or depend materially on domestic law, applicable treaties, or reservations. Article 40(7) is especially important: when the states are already bound by a mutual legal assistance treaty, the corresponding provisions of that treaty ordinarily apply unless the states agree to use Article 40(8) to (31).

Table 2.

Comparative Classification of Cross-Border Stored Electronic Evidence Safeguards

Category	UN Cybercrime Convention	Budapest framework	EU electronic-evidence framework
Jurisdictional and cooperation nexus	P: Arts 3, 5, 22, 35, 40(6)-(7), 42, and 44 distribute scope, offence jurisdiction, territorial limits, and the applicable MLA route.	P: parent-Convention jurisdiction, territorial safeguards, declarations, and procedure-specific party controls.	E: the order, issuing state, enforcing state, provider connection, and territorial conditions are specified.
Competent authority	P: Art 40(12) mandates central authorities and Art 41 a 24/7 contact, but issuing, validating, and executing roles remain substantially domestic.	E: procedure-specific issuing, receiving, and contact-point rules.	E: issuing, validating, enforcing, and provider-facing authorities are specified.

Category	UN Cybercrime Convention	Budapest framework	EU electronic-evidence framework
Specificity	P: Art 42(3) expressly defines preservation-request content. For access and disclosure, Art 40(15), applied through Art 44(2), supplies default content requirements, but an applicable MLA treaty or domestic law may govern.	E: procedure-specific request and certificate content.	E: production and preservation orders and certificates have specified content.
Necessity and time sensitivity	P: Art 42(3)(e) states necessity for preservation, and Art 44(3) requires expedited response in limited cases. The rules are procedure-specific rather than a general test for every request.	P: expedited preservation and urgency rules are expressly stated, but they apply to defined procedures rather than as a general necessity test for every request.	E: necessity conditions and deadlines for production and preservation orders.
Proportionality	P: Art 24 requires proportionality, while domestic law supplies the operational test and limits.	P: Convention safeguards and domestic implementation supply the test.	E: express necessity and proportionality controls, with data-category distinctions.
Independent review	P: Art 24 refers to judicial or other independent review and an effective remedy as appropriate under domestic law.	P: review depends on the procedure and domestic implementation.	E: judicial issue or validation and effective-remedy provisions are specified.
Data protection and use	P: Arts 36 and 40(19) regulate transfer, onward transfer, and later use, while retention, sensitive-data rules, and remedies remain materially domestic.	E: Art 14 of the Second Protocol contains detailed transfer and use safeguards.	E: Regulation 2023/1543, the GDPR, and Directive 2016/680 provide detailed controls.
Preservation	E: Arts 25 and 42 provide expedited preservation; Art 42 requires at least 60 days and generally excludes dual criminality, subject to Art 42(5).	E: expedited preservation and partial traffic-data disclosure procedures.	E: European Preservation Orders and related provider obligations.

Category	UN Cybercrime Convention	Budapest framework	EU electronic-evidence framework
Access and disclosure	P: Art 44 authorises requests, but Art 44(2), Art 35, and Art 40(7) make execution dependent on applicable instruments and law.	E: defined mutual-assistance and provider-disclosure procedures.	E: European Production Orders, notification, and enforcement procedures.
Endpoint functions (separate subcodes)	Request response - P: Art 40(21)-(28) addresses refusal, reasons, postponement, consultation, and conditions, but Art 40(7) may place the request under another MLA treaty. Provider or affected-person remedies - P: Art 24 makes independent review and effective remedies dependent on domestic law. Interstate disputes - P: Art 63 provides a separate route subject to Art 63(3) reservations.	Request response - P: conditions, refusal, confidentiality, and procedural limits are addressed but remain partly treaty-, declaration-, or domestic-law-dependent. Provider or affected-person remedies - P: Convention Art 15 and Second Protocol Arts 13-14 rely materially on domestic implementation. Interstate disputes - N/A: not assessed as part of the selected Budapest evidence-procedure cluster.	Request response - E: notification, objections, compliance, and enforcement limits are specified. Provider or affected-person remedies - E: provider and affected-person remedies are expressly stated. Interstate disputes - N/A: not part of the selected EU e-evidence instrument cluster.

Note. Classification is based on official legal texts. E, P, N, and N/A have the meanings stated in Table 1. The EU and Budapest columns describe instrument clusters rather than single instruments. The endpoint row reports request response, provider or affected-person remedies, and interstate settlement separately. The table records specificity at the selected level of aggregation, not effectiveness, legitimacy, or the quality of domestic implementation.

The absence of N codes in the nine common functional categories follows from the design of the comparison. Those categories were drawn from concerns that the three selected frameworks address in some form, so the absence of N should not be read as independent evidence that every sovereignty, procedural-rights, or data-protection concern has been comprehensively covered. The endpoint functions are treated separately, and N/A is used where interstate settlement is not part of the selected Bu-

dapest or EU evidence-procedure cluster. At the selected level of aggregation, the EU instrument cluster contains the highest degree of textual and institutional specificity. That result partly reflects its combination of several interlocking instruments within a shared regional legal order. The Budapest framework is operationally specific for defined procedures but still relies on the parent Convention and domestic law. Its necessity and time-sensitivity category is therefore coded P because the urgency rules attach to particular procedures rather than to a general test for every request. The UN Convention is open to global participation but leaves more institutional and procedural variation to national systems. The comparison consequently supports a claim about legal specificity at the chosen level of aggregation, not a ranking of practical effectiveness or rights protection.

Three points are especially important when the Convention is applied. First, Article 22 concerns jurisdiction over offences; it is not, by itself, authority to compel or obtain evidence abroad. The cooperation analysis must also consider Articles 3 and 35, the sovereignty limit in Article 5, the applicable-treaty rule in Article 40(6) and (7), and the territorial structure of Articles 42 and 44. Second, Article 42(3) specifies the content of a preservation request. By contrast, the content requirements for an Article 44 access or disclosure request arise mainly through Article 40(15), applicable treaties, and domestic law. Third, Article 44(3) requires an expedited response to an access or disclosure request in specified circumstances; preservation itself is governed by Articles 25 and 42.

Preservation and disclosure should not be treated as equivalent. Preservation secures specified data against loss while an authority prepares or assesses a later request. Article 42 generally excludes dual criminality as a condition for preservation, subject to the reservation permitted by Article 42(5), and requires preservation for at least 60 days, with the possibility of an extension request. Article 43 creates a separate route when preserved traffic data show that another service provider took part in the communication. Disclosure goes further because it exposes or transfers information. It therefore calls for closer scrutiny of authority, dual criminality where applicable, necessity, proportionality, review, privilege, personal-data protection, onward transfer, and permitted use [21, pp. 58-64; 27].

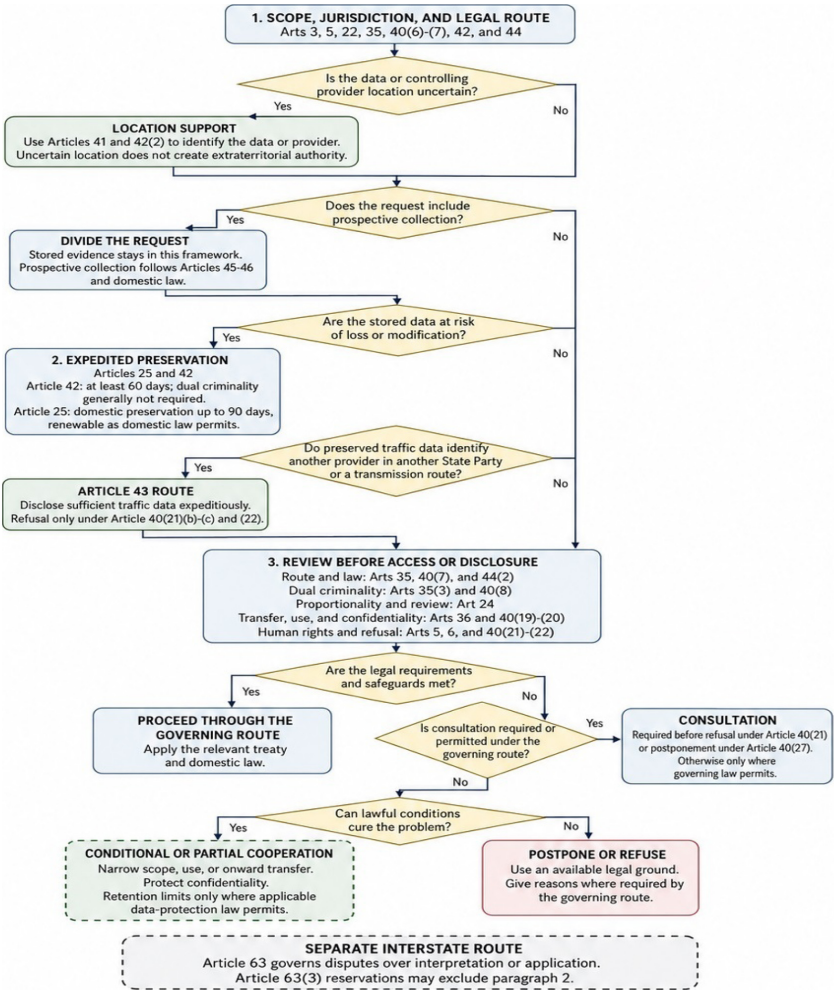


Fig. 1. Proposed Sovereignty-Compatible Stored Electronic Evidence Decision Framework. Rectangles show screening or response stages; diamonds show decision points; and dashed boxes identify steps whose content depends on applicable domestic or international law. The sequence covers scope, jurisdiction and the governing legal route; location support; separation of stored and prospective collection; expedited preservation; the Article 43 traffic-data route; review before access or disclosure; consultation; conditional or partial cooperation; postponement or refusal; and the separate Article 63 interstate-dispute route. MLA means mutual legal assistance.

At the 7 August 2026 status check, Azerbaijan, Qatar, and Viet Nam were the three parties, and each had excluded Article 63(2) through an Article 63(3) reservation [29]. The Article 43 route is mandatory when its conditions are met: sufficient traffic data shall be disclosed expeditiously, subject only to the limited grounds incorporated by Article 43(2), namely Article 40(21)(b)-(c) and (22).

Figure 1 starts with the Convention's substantive scope, offence jurisdiction, sovereignty limits, and the governing mutual-assistance route. Where the location of the data or controlling provider is uncertain, the requesting state may use the Article 41 network and Article 42(2) to seek information about the location of the stored data and, where appropriate, the service provider before selecting the cooperation route. Uncertain location does not itself create authority to exercise public functions in another state. If a request combines stored and prospective collection, the two parts are separated: the stored component remains within this framework, while the prospective component follows Articles 45 and 46 and the requested state's domestic law. Where stored data are vulnerable to loss or modification, Articles 25 and 42 support expedited preservation. The next decision concerns Article 43. If the preserved traffic data identify another provider or transmission route, the requested state shall expeditiously disclose enough traffic data to identify that provider and the transmission path, unless one of the limited refusal grounds incorporated by Article 43(2) applies. The request then moves to the ordinary access or disclosure review. That review considers the governing treaty and domestic law, dual criminality under Articles 35(3) and 40(8) where relevant, proportionality and review, transfer and later-use safeguards under Articles 36 and 40(19), confidentiality under Article 40(20), and the refusal grounds in Article 40.

The boundary between stored and real-time data turns on function, not simply on the label attached to the request. Historical traffic records, stored messages, account files, and subscriber information fall within the present analysis. A request that also seeks prospective traffic collection, continuing location data, or interception of communications must be divided because the real-time component is governed by Articles 45 or

46 and by the requested state's domestic law. Treating the entire request as 'stored' would avoid a materially different legal threshold.

When a request satisfies the relevant legal requirements, it may proceed through the governing cooperation route. A defect does not invariably trigger consultation under Article 40. Paragraph 28 requires the requested state to consult before refusing a request under paragraph 21 or postponing execution under paragraph 27. In other circumstances, consultation is available only where the governing treaty, domestic law, or agreement between the states permits it. If lawful conditions can cure a problem, Articles 36 and 40(19), (20), and (28) may support conditional or partial cooperation, for example by narrowing the category or period of data, limiting use or onward transfer, or protecting confidentiality. A retention limit may be imposed only where it is required or permitted by applicable domestic or international data-protection law; the Convention does not create a general standalone retention period for disclosed evidence. If the problem cannot lawfully be cured, the requested state may postpone or refuse assistance on an available ground and, where the governing route requires it, give reasons. Article 63 remains separate because it concerns disputes between states over the interpretation or application of the Convention, not routine review of an individual evidence request.

Discussion

The comparison leads to a straightforward conclusion: the Convention addresses the core legal elements identified in the analysis, but it does not arrange them in a single operational sequence. A request may satisfy one provision and still be defective under another. Article 42 may support urgent preservation, for example, while Articles 24, 35, 36, 40, and 44 continue to govern the legal route, later access, transfer, and use. The proposed framework makes these dependencies easier to see. It also guards against treating Article 22 as a complete evidence-jurisdiction rule or Article 44(3) as a preservation power. Sovereignty is therefore neither reducible to server location nor an automatic reason to reject cooperation.

Safeguards do not transfer neatly from one legal system to another. The EU framework rests on mutual recognition, shared legal institutions, and detailed rules on enforcement and remedies. The Budapest framework uses defined procedures among parties to an established treaty. The UN Convention, by contrast, seeks global participation across legal systems with widely different judicial capacity, data-protection rules, provider regulation, and access to remedies. Comparator safeguards can help clarify implementation, but they cannot be treated as unexpressed treaty obligations. The Malabo Convention offers a useful reminder that regional cybercrime instruments may emphasise harmonisation, data protection, and capacity-building without reproducing European production-order mechanisms. For that reason, the proposed framework uses comparator safeguards as practical guidance, not as a demand that every state adopt the same institutions or legal forms.

In practical terms, the framework favours measured cooperation over an immediate choice between complete disclosure and complete refusal. The first step is to determine whether another mutual-assistance treaty supplies the controlling procedure under Article 40(7). Where Article 40 applies, paragraph 28 requires consultation before refusal under paragraph 21 or postponement under paragraph 27, so that the states can consider whether lawful conditions would permit assistance. Consultation in other situations depends on the governing treaty, domestic law, or agreement between the states. Conditions may concern scope, confidentiality, use, privilege, or onward transfer. They may include retention limits only where applicable domestic or international data-protection law authorises or requires them. Paragraph 17 requires execution under the requested state's law and observance of a requested procedure only when that procedure is compatible with the same law; it should not be treated as an independent source of every possible condition. Consider a request for six months of stored content when only one month is linked to the offence. The requested state may preserve the account, disclose the relevant period subject to lawful use restrictions, and consult on the remainder where the governing route permits.

Uneven implementation remains a serious prospective risk. Articles 24 and 40 leave substantial details of proportionality, review, execution,

and remedies to domestic law, so formally similar safeguards may work very differently from one state to another. Where judicial independence is weak, speech offences are broad, remedies are limited, or data-protection oversight is ineffective, those safeguards may offer less practical restraint. Article 22(2)(a) may also facilitate jurisdictional shopping by allowing a state to rely on harm to one of its nationals even when the conduct and the person concerned are abroad [23]. A requesting authority may try to rely on the most permissive legally available cooperation route, seek parallel assistance from several jurisdictions, or present a political or expressive offence as an ordinary serious-crime request. Articles 5, 6, 24, and 40(22) provide relevant safeguards, but their value will depend on meaningful scrutiny by the requested state. Requests involving journalism, cybersecurity research, political opposition, protected expression, or a politically framed offence should therefore be examined for purpose, dual criminality, foreseeable human-rights consequences, and the availability of an effective remedy [4; 10; 19]. These are prospective implementation risks, not empirical findings about the current parties' practice.

Ratification alone will not settle these issues. At the 7 August 2026 status check, the Convention had 79 signatories and three parties (Azerbaijan, Qatar, and Viet Nam), each of which had excluded Article 63(2) through an Article 63(3) reservation [29]. This small early sample cannot support conclusions about the parties' motives or the Convention's long-term viability. It does, however, show why future research should examine reservation practice, declarations, designated authorities, and implementing legislation alongside the treaty text. Viet Nam's declaration that the Convention is non-self-executing also illustrates how domestic constitutional and statutory rules may shape implementation [29]. For routine disagreements over a request, consultation under Article 40 is likely to provide a more immediate mechanism than Article 63. The latter concerns disputes over treaty interpretation or application, and its arbitration and possible ICJ route may be unavailable because of a reservation.

The study has six limitations. First, the Convention has not entered into force, so this ex ante analysis cannot establish how states, courts, or

providers will behave. Second, the classification measures legal specificity rather than effectiveness. Its categories and final codes represent one reasoned interpretation of the instruments and may be challenged by other scholars or by states during implementation. Third, the literature search was targeted rather than systematic and may have missed relevant work outside the selected sources, languages, or search terms. Fourth, the formal comparators are functionally European and do not represent every African, Asian, Latin American, or Eurasian approach. Fifth, the units compared are asymmetric: the Budapest and EU columns combine instrument clusters, whereas the UN column evaluates a global convention before national implementation practice has developed. The results must therefore be read as a comparison of specificity at the selected level of aggregation, not as a ranking of complete legal regimes. Sixth, the focus on stored data excludes the distinct safeguards that govern real-time traffic collection and interception. Future research should test the framework against implementing laws, real request files, judicial decisions, provider objections, state declarations, and mixed stored and prospective requests after entry into force.

Conclusion

This study examined how the UN Cybercrime Convention is designed to reconcile cross-border access to stored electronic evidence with state sovereignty. RQ1 shows that lawful cooperation requires more than offence jurisdiction under Article 22. It also requires attention to the Convention's scope under Articles 3 and 35, respect for sovereignty and human rights under Articles 5 and 6, identification of the governing route under Article 40(6) and (7), and application of the procedural safeguards in Articles 24 to 28, 36, and 40 to 44. RQ2 shows how the Budapest and EU frameworks clarify the value of defined authorities, procedure-specific request content, independent validation, provider-facing objections, and effective remedies. Those safeguards may inform implementation, but they cannot be imported as new treaty duties.

For RQ3, the article proposes a Sovereignty-Compatible Stored Electronic Evidence Decision Framework. It is a doctrinal and nor-

mative synthesis, not an empirically validated model. The framework first screens scope, jurisdiction, territorial limits, and the applicable mutual-assistance route. It then separates urgent preservation from later disclosure, includes the Article 43 traffic-data pathway, distinguishes stored evidence from real-time collection, and directs authorities toward full, conditional, or partial cooperation, postponement, refusal, or consultation. Interstate dispute settlement under Article 63 remains a separate and exceptional route.

The stated objective is therefore achieved: the analysis develops and justifies a sovereignty-compatible decision sequence for stored electronic evidence and identifies the limits of Budapest and EU mechanisms as comparative implementation guidance rather than sources of obligations under the UN Convention. These conclusions remain subject to legal and temporal limits. Domestic safeguards, judicial capacity, political incentives, provider compliance, reservations, and the quality of remedies will vary across states. The comparative findings also reflect the selected level of aggregation: the Budapest and EU columns combine instrument clusters, whereas the UN column evaluates treaty design before national implementation practice has developed.

Once the Convention enters into force, the Conference of the States Parties and national legislators should give priority to guidance on the Article 40(7) treaty interface, authorisation, proportionality, independent review, dual criminality, conditional assistance, provider objections, reasons for refusal, and protection against politically motivated requests. On the normative account developed here, cross-border access is sovereignty-compatible when it rests on clear authority, remains limited to what is necessary, allows meaningful review, protects personal data, and respects the requested state's sovereign legal functions.

Conflict of interest information. The authors declare no conflict of interest.

Sponsorship information. The study had no sponsorship.

Supplementary Appendix

Table S1.

Category-Level Provision Mapping and Classification Matrix

Framework	Category	Principal provision(s)	Final code	Coding rationale
UN Cybercrime Convention	Jurisdictional and cooperation nexus	Arts 3, 5, 22, 35, 40(6)-(7), 42, 44	**P**	Scope, offence jurisdiction, sovereignty limits, territorial links, and the governing cooperation route are spread across several provisions and may depend on another MLA treaty.
UN Cybercrime Convention	Competent authority	Arts 40(12), 41	**P**	Central authorities and a 24/7 contact are required, but issuing, validating, and executing roles remain substantially domestic.
UN Cybercrime Convention	Specificity	Arts 42(3), 40(15), 44(2)	**P**	Preservation-request content is express. Access-request content follows the default Article 40 route only where an applicable treaty or domestic law does not govern.
UN Cybercrime Convention	Necessity and time sensitivity	Arts 42(3)(e), 44(3)	**P**	Necessity and expedited response are stated for particular procedures rather than as a general test for every request.
UN Cybercrime Convention	Proportionality	Art 24	**P**	Proportionality is required, but the operational test, limits, and remedies are mainly supplied by domestic law.
UN Cybercrime Convention	Independent review	Art 24	**P**	Judicial or other independent review and an effective remedy apply as appropriate under domestic law.
UN Cybercrime Convention	Data protection and use	Arts 36, 40(19)	**P**	Transfer, onward transfer, and later use are regulated, while retention, sensitive-data rules, and remedies remain materially domestic.
UN Cybercrime Convention	Preservation	Arts 25, 42	**E**	The Convention provides express domestic and international preservation procedures, a minimum 60-day period, and a defined dual-criminality rule.
UN Cybercrime Convention	Access and disclosure	Arts 35, 40(7), 44	**P**	Article 44 authorises requests, but execution depends materially on applicable instruments and the requested state's law.
UN Cybercrime Convention	Endpoint functions (separate subcodes)	Arts 24, 40(21)-(28), 63	**P / P / P**	Request response is partly dependent on the applicable MLA route under Art 40(7); provider or affected-person remedies depend materially on domestic law under Art 24; interstate settlement is express in Art 63 but remains subject to Art 63(3) reservations.

Framework	Category	Principal provision(s)	Final code	Coding rationale
Budapest framework	Jurisdictional and cooperation nexus	Convention Arts 22, 27, 29-32; Second Protocol Arts 6-8	**P**	Jurisdiction, mutual assistance, transborder access, and direct-provider routes are distributed and remain affected by party declarations and domestic law.
Budapest framework	Competent authority	Convention Arts 27(2), 35; Second Protocol authority provisions	**E**	Central or receiving authorities and 24/7 contact points are expressly assigned for the relevant procedures.
Budapest framework	Specificity	Convention Arts 27(4), 29(2), 31(4); Second Protocol Arts 6-8	**E**	The relevant procedures specify the authority, facts, offence, requested data, purpose, and supporting information.
Budapest framework	Necessity and time sensitivity	Convention Arts 29-31; Second Protocol expedited procedures	**P**	Urgency and expedited handling are express but tied to defined procedures rather than to one general necessity test for every request.
Budapest framework	Proportionality	Convention Art 15; Second Protocol Art 13	**P**	General safeguards require proportionality, but operational tests and limits depend substantially on domestic implementation.
Budapest framework	Independent review	Convention Art 15; Second Protocol Art 13	**P**	Review and remedies depend on the particular procedure and the implementing law of each party.
Budapest framework	Data protection and use	Second Protocol Art 14; Convention Art 15	**E**	The Protocol states detailed controls for transfer, purpose, use, retention, onward transfer, sensitive data, and remedies.
Budapest framework	Preservation	Convention Arts 16, 29-30	**E**	Domestic and cross-border preservation, together with limited disclosure of preserved traffic data, are expressly regulated.
Budapest framework	Access and disclosure	Convention Arts 18, 31-32; Second Protocol Arts 6-8	**E**	Production, mutual-assistance access, consent-based access, and provider-disclosure procedures are defined.

Framework	Category	Principal provision(s)	Final code	Coding rationale
Budapest framework	Endpoint functions (separate subcodes)	Convention Arts 15, 27-28; Second Protocol Arts 13-14	**P / P / N/A**	Request response, conditions, refusal, and confidentiality are addressed but remain partly treaty-, declaration-, or domestic-law-dependent. Provider and individual remedies depend materially on domestic implementation. Interstate settlement is outside the selected evidence-procedure cluster.
EU electronic-evidence framework	Jurisdictional and cooperation nexus	Regulation 2023/1543; Directive 2023/1544	**E**	The issuing state, enforcing state, provider connection, designated establishment or representative, and order routes are expressly defined.
EU electronic-evidence framework	Competent authority	Regulation 2023/1543 Arts 4-7, 16; Directive 2023/1544	**E**	Issuing, validating, enforcing, and provider-facing roles are assigned by the legislation.
EU electronic-evidence framework	Specificity	Regulation 2023/1543 Arts 8-10 and annexed certificates	**E**	Production and preservation orders and their certificates contain prescribed information.
EU electronic-evidence framework	Necessity and time sensitivity	Regulation 2023/1543 Arts 5-6, 10-12	**E**	Necessity conditions and response deadlines are stated for production and preservation orders.
EU electronic-evidence framework	Proportionality	Regulation 2023/1543 Arts 5-6	**E**	The Regulation requires express necessity and proportionality assessments, including distinctions between data categories.
EU electronic-evidence framework	Independent review	Regulation 2023/1543 Arts 4, 18	**E**	Judicial issuance or validation and effective-remedy provisions are specified.
EU electronic-evidence framework	Data protection and use	Regulation 2023/1543; GDPR; Directive 2016/680	**E**	The combined framework contains detailed rules on processing, purpose, use, transfer, security, and remedies.
EU electronic-evidence framework	Preservation	Regulation 2023/1543 preservation-order provisions	**E**	European Preservation Orders, certificates, deadlines, and related provider obligations are expressly regulated.

Framework	Category	Principal provision(s)	Final code	Coding rationale
EU electronic-evidence framework	Access and disclosure	Regulation 2023/1543 production and enforcement provisions	**E**	European Production Orders, notification, compliance, and enforcement procedures are defined.
EU electronic-evidence framework	Endpoint functions (separate subcodes)	Regulation 2023/1543 objection, enforcement, and remedy provisions; Directive 2023/1544	**E / E / N/A**	Request response and enforcement limits are express, as are provider and affected-person remedies. Interstate settlement is not part of the selected EU e-evidence instrument cluster.

Note. The matrix maps the principal provisions supporting each code. E means express; P means materially dependent; N means absent; and N/A is used only where interstate settlement falls outside the selected instrument cluster. Endpoint codes are ordered as follows: request response; provider or affected-person remedies; interstate settlement.

References

1. Abraha, H. H. (2020). Regulating law enforcement access to electronic evidence across borders: The United States approach. *Information & Communications Technology Law*, *29*(3), 324–353. https://doi.org/10.1080/13600834.2020.1794617. EDN: https://elibrary.ru/AXPXAA
2. Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, *29*(2), 118–153. https://doi.org/10.1093/ijlit/eaab001. EDN: https://elibrary.ru/XVNEUR
3. African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
4. Barber, I. A., & Kumar, S. (2024). Learning from the ground up: Lessons from civil society engagement in addressing the human rights implications of cybercrime legislation. *Journal of Cyber Policy*, *9*(2), 131–148. https://doi.org/10.1080/23738871.2023.2240331. EDN: https://elibrary.ru/PHJMOC
5. Carrera, S., Stefan, M., & Mitsilegas, V. (2020). *Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*. Centre for

European Policy Studies. https://www.ceps.eu/ceps-publications/cross-border-data-access-in-criminal-proceedings-and-the-future-of-digital-justice

6. Christakis, T., & Terpan, F. (2021). EU-US negotiations on law enforcement access to data: Divergences, challenges and EU law procedures and options. *International Data Privacy Law*, *11*(2), 81–106. https://doi.org/10.1093/idpl/ipaa022. EDN: https://elibrary.ru/YULNZE
7. Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
8. Council of Europe. (2021). *Explanatory report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). https://rm.coe.int/second-additional-protocol-to-the-convention-on-cybercrime-explanatory/1680a2aef1
9. Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
10. Cybersecurity Tech Accord. (2024, August 8). *Open letter from civil society and industry stakeholders on the final draft of the Convention on Cybercrime*. https://cybertechaccord.org/uploads/prod/Final-Draft-Cybercrime-Convention-Multistakeholder-Statement.pdf
11. European Commission. (2018, April 17). *Frequently asked questions: New EU rules to obtain electronic evidence* (MEMO/18/3345). https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
12. European Parliament & Council of the European Union. (2014). Directive 2014/41/EU regarding the European Investigation Order in criminal matters. *Official Journal of the European Union*, *L 130*, 1–36. https://eur-lex.europa.eu/eli/dir/2014/41/oj
13. European Parliament & Council of the European Union. (2016a). Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for law-enforcement purposes. *Official Journal of the European Union*, *L 119*, 89–131. https://eur-lex.europa.eu/eli/dir/2016/680/oj
14. European Parliament & Council of the European Union. (2016b). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*, *L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
15. European Parliament & Council of the European Union. (2023a). Directive (EU) 2023/1544 laying down harmonised rules on designated establishments and legal representatives for gathering electronic evidence in criminal proceedings. *Official Journal of the European Union*, *L 191*, 181–190. https://eur-lex.europa.eu/eli/dir/2023/1544/oj

16. European Parliament & Council of the European Union. (2023b). Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings. *Official Journal of the European Union*, *L 191*, 118–180. https://eur-lex.europa.eu/eli/reg/2023/1543/oj
17. Global Privacy Assembly. (2021). *Resolution on government access to data, privacy and the rule of law: Principles for governmental access to personal data held by the private sector for national security and public safety purposes*. https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf
18. Hakmeh, J. (2024). The UN convention on cybercrime: A milestone in cybercrime cooperation? *Journal of Cyber Policy*, *9*(2), 125–130. https://doi.org/10.1080/23738871.2024.2441549. EDN: https://elibrary.ru/AHHJXQ
19. Human Rights Watch. (2024, October 21). *EU: Member states should vote 'No' on UN Cybercrime Treaty*. https://www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cybercrime-treaty
20. Kuckartz, U., & Rädiker, S. (2023). *Qualitative content analysis: Methods, practice and using software*. SAGE. https://uk.sagepub.com/en-gb/eur/qualitative-content-analysis/book279751
21. Mason, S., & Seng, D. (2021). The foundations of evidence in electronic form. In S. Mason & D. Seng (Eds.), *Electronic evidence and electronic signatures* (5th ed., pp. 51–84). University of London Press. https://doi.org/10.14296/2108.9781911507246
22. Organisation for Economic Co-operation and Development. (2022). *OECD Declaration on Government Access to Personal Data Held by Private Sector Entities* (OECD/LEGAL/0487). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487
23. Scher-Zagier, E. (2024). Jurisdictional creep: The UN Cybercrime Convention and the expansion of passive personality jurisdiction. *SSRN*. https://doi.org/10.2139/ssrn.4957176
24. Sukumar, A., & Basu, A. (2024). Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order. *Journal of Cyber Policy*, *9*(2), 256–287. https://doi.org/10.1080/23738871.2024.2436591
25. United Nations. (1969). *Vienna Convention on the Law of Treaties*. *United Nations Treaty Series*, *1155*, 331. https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf
26. United Nations. (2020). *Countering the use of information and communications technologies for criminal purposes* (A/RES/74/247). https://docs.un.org/en/A/RES/74/247
27. United Nations. (2024). *United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes* (A/RES/79/243, annex). https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

28. United Nations Counter-Terrorism Committee Executive Directorate. (2022). *The state of international cooperation for lawful access to digital evidence*. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf
29. United Nations Treaty Collection. (n.d.). *United Nations Convention against Cybercrime: Status of treaties*. Retrieved August 7, 2026, from https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en
30. United States Congress. (2018). *Clarifying Lawful Overseas Use of Data Act*, Pub. L. No. 115-141, div. V, *132 Stat.* 1213. https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf
31. Vardanyan, L., & Kocharyan, H. (2022). Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: Main obstacles and challenges. *European Studies*, *9*(2), 110–132. https://doi.org/10.2478/eustu-2022-0016. EDN: https://elibrary.ru/FZGOYT
32. Vardanyan, L., Kocharyan, H., Hamuľák, O., & Kerikmäe, T. (2023). Digital sovereignty in the EU: Searching for legal mechanisms for marking the borders. In D. Ramiro Troitiño, T. Kerikmäe, & O. Hamuľák (Eds.), *Digital development of the European Union* (pp. 219–234). Springer, Cham. https://doi.org/10.1007/978-3-031-27312-4_14

DATA ABOUT THE AUTHORS

Bridget Silver Aziaka, Master of Laws (LLM) in International Dispute Settlement
Center for International Dispute Settlement
Geneva, Switzerland
Bridgetchiaziaka20@gmail.com

Uchenna Isaac Nwokorie, LLB
Okocha & Okocha Legal Practitioners
Port Harcourt, Nigeria
uchennanwokonig@gmail.com

Chukwu Kingsley Ibiso, BSc in Mass Communication, Public Relations Officer
Babalakin & Co. Legal Practitioners
Port Harcourt, Nigeria
Kingsibisochuks@gmail.com

Поступила 10.07.2026 Received 10.07.2026
После рецензирования 13.08.2026 Revised 13.08.2026
Принята 17.08.2026 Accepted 17.08.2026