

Digital Evidence and the Digital Procedural Divide: Rethinking Equality in Global Cybercrime Adjudication

¹Hamdani Padli, ¹Nilam Sukmawati, ²Ilhamda Fattah Kaloko

¹Faculty of Sharia, UIN Sulthan Thaha Saifuddin Jambi, Indonesia

²Faculty of Law, Universitas Maritim Raja Ali Haji, Indonesia

Corresponding author: hamdanipadli@uinjambi.ac.id.

Received: June 02, 2026 | Revised: June 29, 2026; July 24, 2026 | Accepted: July 30, 2026

Abstract

The rapid expansion of digital technologies has transformed evidentiary governance in cybercrime cases, where electronic evidence is increasingly stored beyond the territorial jurisdiction of investigating states. Although various international legal instruments have been developed to facilitate access to cross-border digital evidence, existing scholarship has primarily focused on issues of jurisdiction, digital sovereignty, and international cooperation. This article argues that a more fundamental challenge lies in unequal access to digital evidence and its implications for procedural inequality in cybercrime adjudication. Employing normative legal research with a transnational legal approach, this study conducts a conceptual analysis of international legal instruments, regulations governing electronic evidence, and scholarly literature on cybercrime and digital governance. The analysis combines doctrinal, comparative, and critical methods to examine the relationship between access to digital evidence and procedural equality. The findings reveal that jurisdictional fragmentation, the dominance of global digital platforms as data gatekeepers, and disparities in investigative capacities among states have created structural inequalities in access to cross-border electronic evidence. To explain this phenomenon, the article develops the concept of the Digital Procedural Divide, defined as a structural disparity in the ability of states and legal actors to obtain, authenticate, and utilize digital evidence in criminal proceedings. The study demonstrates that unequal access to digital evidence may undermine the principles of equality before the law, due process, and access to justice. It concludes that global digital evidence governance should be reoriented from a narrow focus on investigative efficiency toward the promotion of procedural equality in cybercrime adjudication.

Keywords: Cross-Border Digital Evidence; Digital Procedural Divide; Cybercrime Adjudication; Procedural Equality; Access to Justice.

Abstrak

Perkembangan teknologi digital telah mengubah tata kelola pembuktian dalam perkara kejahatan siber, di mana bukti elektronik semakin sering tersimpan di luar yurisdiksi negara yang melakukan penyidikan. Meskipun berbagai instrumen hukum internasional telah dikembangkan untuk memfasilitasi akses terhadap bukti digital lintas negara, sebagian besar penelitian masih berfokus pada isu yurisdiksi, kedaulatan digital, dan kerja sama internasional. Artikel ini berargumen bahwa persoalan yang lebih mendasar adalah ketimpangan akses terhadap bukti digital yang berimplikasi pada ketidaksetaraan prosedural dalam adjudikasi kejahatan siber. Penelitian ini menggunakan metode hukum normatif dengan pendekatan hukum transnasional dan analisis konseptual terhadap instrumen hukum internasional, regulasi terkait bukti elektronik, serta literatur mengenai

kejahatan siber dan tata kelola digital. Analisis dilakukan secara doktrinal, komparatif, dan kritis untuk mengkaji hubungan antara akses terhadap bukti digital dan prinsip kesetaraan prosedural. Hasil penelitian menunjukkan bahwa fragmentasi yurisdiksi, dominasi platform digital global sebagai pengendali data, dan ketimpangan kapasitas investigatif antarnegara telah menciptakan kesenjangan struktural dalam akses terhadap bukti elektronik lintas negara. Untuk menjelaskan fenomena tersebut, artikel ini mengembangkan konsep Digital Procedural Divide, yaitu kesenjangan struktural dalam kemampuan negara dan aktor hukum untuk memperoleh, memverifikasi, dan memanfaatkan bukti digital dalam proses peradilan pidana. Temuan ini menunjukkan bahwa ketimpangan akses terhadap bukti digital berpotensi mengikis prinsip equality before the law, due process, dan access to justice. Artikel ini menyimpulkan bahwa tata kelola bukti digital global perlu direorientasikan dari sekadar efisiensi investigasi menuju kesetaraan prosedural dalam adjudikasi kejahatan siber.

Kata Kunci: Bukti Digital Lintas Negara; Digital Procedural Divide; Adjudikasi Kejahatan Siber; Kesetaraan Prosedural; Akses terhadap Keadilan.



Copyright © 2026 by Author(s)

This work is licensed under a [Creative Commons Attribution 4.0 International License \(CC BY 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/).

Introduction

The rapid expansion of digital technologies has fundamentally transformed both the nature of criminal activity and the mechanisms through which evidence is generated, stored, and accessed. Cybercrime investigations increasingly rely on electronic evidence located outside the territorial jurisdiction of the investigating state, including data stored in cloud infrastructures, social media platforms, encrypted messaging services, and transnational digital ecosystems. As a consequence, criminal adjudication in the digital era is no longer determined solely by domestic procedural law but is increasingly shaped by complex interactions among transnational legal frameworks, private technology companies, and competing claims of digital sovereignty (Kerr, 2022).

The growing dependence on cross-border digital evidence has generated unprecedented challenges for criminal justice systems worldwide. Law enforcement agencies frequently encounter difficulties in accessing electronic evidence located abroad, particularly when such data are controlled by multinational technology corporations operating across multiple jurisdictions. Traditional mechanisms of international cooperation, such as Mutual Legal Assistance Treaties (MLATs), are often criticized for being slow, bureaucratic, and ill-suited to the rapid alteration, deletion, or transfer of digital evidence (Daskal, 2018b). In response, several jurisdictions have introduced new legal instruments intended to facilitate cross-border access to electronic evidence, including the Budapest Convention on Cybercrime, the United States CLOUD Act, and the European Union E-Evidence Regulation (Abraha, 2020; Moise, 2024).

Despite these developments, significant controversy remains regarding the implications of transnational evidence-gathering for due process, privacy protection, and procedural fairness. Existing scholarship has generally evolved along three major strands.

The first strand focuses on questions of jurisdiction and cross-border enforcement. Scholars such as Dan Jerker B. Svantesson, Cedric Ryngaert, and Christopher Kuner have examined how territorial principles of jurisdiction struggle to accommodate digital environments in which data can be simultaneously stored, processed, and accessed across multiple states (Kuner, 2013; Ryngaert, 2025; Svantesson, 2017). Their work demonstrates that the transnational character of digital evidence challenges conventional assumptions regarding territorial sovereignty and legal authority.

The second strand explores the relationship between electronic evidence and fundamental rights, particularly privacy, data protection, and human rights safeguards. Research by Jennifer Daskal, Paul De Hert, Serge Gutwirth, and others highlights the tensions between effective law enforcement and the protection of individual rights when governments seek access to data stored abroad (Daskal, 2018a; Gutwirth & De Hert, 2022). This literature has significantly contributed to debates concerning proportionality, legality, and judicial oversight in transnational digital investigations.

A third strand of scholarship examines the increasing role of technology companies as gatekeepers of digital evidence. Scholars such as Julie E. Cohen, Jack M. Balkin, and Nicolas P. Suzor argue that global digital platforms have become quasi-regulatory actors whose decisions increasingly shape the accessibility, retention, and disclosure of information relevant to criminal proceedings (Balkin, 2018; Cohen, 2019; Suzor, 2019). From this perspective, access to evidence is no longer governed exclusively by public law institutions but is also mediated by private actors exercising substantial influence over digital infrastructures.

While these bodies of literature have substantially advanced understanding of cross-border digital evidence, important gaps remain. Existing studies predominantly conceptualize the problem as one of jurisdictional conflict, international cooperation, privacy protection, or platform governance. Relatively little attention has been paid to the structural inequalities produced by unequal access to digital evidence across different jurisdictions. In particular, current scholarship has not adequately examined how disparities in technological capacity, geopolitical influence, legal infrastructure, and bargaining power vis-à-vis global technology companies affect the ability of states to obtain and utilize electronic evidence in criminal proceedings.

This omission is significant because access to cross-border digital evidence is not distributed equally among states. Governments possessing greater technological resources, stronger diplomatic leverage, and direct cooperation mechanisms with major technology providers often enjoy more efficient access to electronic evidence. By contrast, many developing countries remain dependent upon lengthy and resource-intensive international cooperation procedures (United

Nations Office on Drugs and Crime (UNODC), 2024). Consequently, the practical ability to investigate, prosecute, and adjudicate cybercrime increasingly depends not only upon legal authority but also upon a state's position within the broader architecture of global digital governance.

The unequal distribution of access to digital evidence raises concerns extending beyond efficiency and enforcement. At a deeper level, it challenges fundamental principles of procedural equality and equal access to justice. If some jurisdictions systematically possess greater capacity to secure crucial evidence while others face persistent structural barriers, then the administration of criminal justice may become increasingly shaped by asymmetries of power embedded within global digital infrastructures. Yet this dimension remains largely under-theorized within contemporary cybercrime scholarship.

This article argues that these challenges are best understood through the concept of the Digital Procedural Divide, defined as a structural disparity in the ability of states and litigants to obtain, authenticate, and utilize cross-border digital evidence in criminal proceedings. The article further contends that contemporary debates concerning cross-border digital evidence should move beyond questions of jurisdiction and sovereignty to address broader concerns regarding procedural equality, due process, and access to justice within global cybercrime adjudication.

Accordingly, this study addresses two principal research questions. First, how does the contemporary governance structure of cross-border digital evidence generate procedural inequalities in cybercrime adjudication? Second, how can the concept of the Digital Procedural Divide provide a new analytical framework for understanding the relationship between access to digital evidence, procedural equality, and justice in transnational criminal proceedings?

The article contributes to the literature in three respects. First, it develops the concept of the Digital Procedural Divide as a novel theoretical framework for analyzing inequalities in access to cross-border digital evidence. Second, it bridges previously disconnected literatures on cybercrime adjudication, digital sovereignty, and procedural justice. Third, it reframes cross-border digital evidence as a question not merely of jurisdictional competence but of structural equality within contemporary systems of global criminal justice.

Methodology

This study employs a normative legal research design combined with a transnational legal analysis approach to examine the relationship between cross-border digital evidence and procedural inequality in cybercrime adjudication. A normative approach is appropriate because the central concern of this article lies in the examination of legal norms, institutional frameworks, and

regulatory mechanisms governing access to digital evidence across jurisdictions rather than in the measurement of empirical behavior or individual perceptions (Hutchinson, 2024).

However, given that cross-border digital evidence is generated and controlled within complex digital ecosystems involving states, international organizations, and private technology companies, this study does not confine itself to a purely doctrinal examination of legal texts. Instead, it adopts a transnational legal perspective that recognizes the interaction between domestic law, international legal instruments, private regulatory arrangements, and technological infrastructures in shaping contemporary systems of digital evidence governance (Zumbansen, 2012). This perspective enables a broader understanding of how legal authority and evidentiary access are distributed beyond traditional territorial boundaries.

The research materials consist of three categories of legal and policy sources. The first category includes primary legal materials, namely international and regional instruments governing electronic evidence and cybercrime investigations. These include the Budapest Convention on Cybercrime, the Second Additional Protocol to the Budapest Convention on Enhanced Cooperation and Disclosure of Electronic Evidence, the United States CLOUD Act, the European Union E-Evidence Regulation, and relevant international human rights instruments concerning due process and privacy protections (Moise, 2024; Radoniewicz, 2025).

The second category consists of secondary legal materials, including scholarly literature on cybercrime law, digital evidence, transnational criminal justice, digital sovereignty, platform governance, and procedural fairness. Particular attention is given to studies examining jurisdictional challenges, cross-border data access, and the growing role of private technology companies in criminal investigations (Daskal, 2018a; Suzor, 2019; Svantesson, 2017).

The third category comprises institutional reports, policy papers, and technical assessments published by international organizations, including the United Nations Office on Drugs and Crime (UNODC), the Council of Europe, the European Commission, and other bodies involved in cybercrime governance. These materials provide insight into contemporary challenges surrounding international cooperation, digital evidence collection, and disparities in investigative capacities among states (European Commission, 2018; United Nations Office on Drugs and Crime (UNODC), 2024).

Data are analyzed through qualitative legal analysis using three interconnected stages. First, doctrinal analysis is employed to identify the normative principles governing access to digital evidence across jurisdictions. Second, comparative analysis is used to examine how different legal regimes address issues of jurisdiction, evidence disclosure, and transnational cooperation. Third,

critical legal analysis is applied to evaluate the implications of these frameworks for procedural equality and access to justice (Hutchinson & Duncan, 2012).

Rather than treating cross-border digital evidence solely as a technical problem of international cooperation, this analytical framework seeks to uncover the structural inequalities embedded within contemporary systems of digital evidence governance. Through this approach, the study develops the concept of the Digital Procedural Divide as an analytical framework for explaining disparities in the ability of states and litigants to obtain, authenticate, and utilize digital evidence in transnational criminal proceedings (Pillsbury, 2019). The concept is generated through inductive synthesis of the legal materials and scholarly debates examined throughout the study and is subsequently used to evaluate the implications of cross-border digital evidence for procedural equality in global cybercrime adjudication.

Findings and Discussion

Jurisdictional Fragmentation and the Privatization of Cross-Border Digital Evidence

The emergence of digital technologies has fundamentally disrupted the territorial assumptions that have historically underpinned criminal procedure and evidentiary law. Traditional criminal justice systems were developed on the premise that evidence, suspects, and criminal conduct could generally be located within identifiable territorial boundaries. In the digital environment, however, electronic evidence is frequently generated, transmitted, processed, and stored across multiple jurisdictions simultaneously, creating unprecedented challenges for the exercise of criminal jurisdiction and the collection of evidence (Kerr, 2022). As a result, the territorial nexus that once linked criminal investigations to a specific geographic location has become increasingly difficult to identify and enforce.

This transformation is particularly evident in contemporary cybercrime investigations. Electronic communications, cloud-based documents, social media records, metadata, and transactional logs may involve users located in one country, service providers headquartered in another, and data centers distributed across several additional jurisdictions. The transnational architecture of digital networks means that a single piece of evidence may be subject to multiple and sometimes conflicting legal regimes (Daskal, 2018a). Consequently, determining which state possesses the authority to access, preserve, or disclose digital evidence has become one of the most contested issues in contemporary cybercrime governance.

The inadequacy of territorial jurisdiction in addressing digital evidence has been widely recognized within international legal scholarship. Classical principles of criminal jurisdiction—

particularly territoriality, nationality, and protective jurisdiction—were designed for a legal environment in which the location of persons, objects, and conduct could be reasonably identified (Ryngaert, 2025). In cyberspace, however, data possess a fundamentally deterritorialized character. Information can be fragmented across multiple servers, mirrored in different jurisdictions, and transferred instantaneously without regard to national borders. This technological reality has generated what scholars describe as a jurisdictional mismatch between territorially bounded legal systems and globally distributed digital infrastructures (Svantesson, 2017).

The practical consequences of this mismatch are reflected in the persistent difficulties surrounding cross-border access to electronic evidence. For decades, states have relied on Mutual Legal Assistance Treaties (MLATs) as the principal mechanism for obtaining evidence located abroad. Although MLATs remain an important instrument of international cooperation, they have been criticized as being excessively slow and procedurally burdensome in the context of cybercrime investigations (United Nations Office on Drugs and Crime (UNODC), 2024). Digital evidence is often highly volatile; data can be altered, deleted, encrypted, or transferred within minutes. Delays of several months or even years in obtaining evidence through traditional mutual assistance channels may therefore significantly undermine the effectiveness of criminal investigations and prosecutions.

Recognizing these limitations, states and international organizations have increasingly sought alternative mechanisms to facilitate access to cross-border digital evidence. One of the most influential developments has been the expansion of the regulatory framework established under the Convention on Cybercrime (Budapest Convention), particularly through the adoption of the Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence (Council of Europe, 2022). The Protocol seeks to streamline procedures for obtaining subscriber information, facilitating direct cooperation with service providers, and enhancing international cooperation mechanisms. Similarly, the United States enacted the CLOUD Act in 2018, authorizing certain forms of extraterritorial access to data held by service providers under U.S. jurisdiction and creating a framework for executive agreements with foreign governments (Daskal, 2018b). The European Union has likewise introduced the E-Evidence Regulation, which enables judicial authorities within member states to issue cross-border production and preservation orders directly to service providers operating within the European digital market (Kuczyńska, 2024; Sachoulidou, 2024).

While these regulatory innovations are often presented as solutions to the challenges of digital evidence collection, they simultaneously reveal a deeper transformation in the governance of criminal evidence. Access to digital evidence is increasingly mediated not only by states and

international legal instruments but also by private technology companies that own and control the infrastructures through which digital information is generated and stored. Unlike conventional forms of physical evidence, electronic evidence frequently remains under the custody of private service providers, including cloud computing companies, social media platforms, messaging applications, and internet service providers (Kuner, 2013). Consequently, the practical accessibility of evidence often depends less on territorial jurisdiction and more on the willingness and capacity of private entities to respond to governmental requests.

This development has contributed to what may be described as the privatization of evidentiary access. Traditionally, the collection and disclosure of criminal evidence were functions exercised predominantly by public authorities operating within clearly defined legal frameworks. In the contemporary digital environment, however, technology companies increasingly occupy a pivotal position between states and evidence. These companies determine data retention policies, establish internal procedures for responding to governmental requests, implement encryption technologies, and define the technical conditions under which information may be accessed or disclosed (Cohen, 2019). As a result, private actors have acquired substantial influence over the practical operation of criminal justice systems, despite not being formally integrated into traditional structures of public authority.

The growing role of technology companies in evidentiary governance has generated significant implications for state sovereignty. Although states continue to possess formal legal authority over criminal investigations, their ability to exercise that authority increasingly depends upon cooperation from transnational corporations operating beyond the effective reach of domestic legal systems. This phenomenon has led several scholars to argue that digital platforms have evolved into quasi-regulatory institutions capable of shaping the implementation of legal norms across multiple jurisdictions (Balkin, 2018; Suzor, 2019). The power to control access to information has effectively become a form of governance in its own right, one that operates alongside and sometimes independently of conventional state authority.

The fragmentation of jurisdiction and the privatization of evidentiary access therefore represent interconnected dimensions of a broader transformation in global criminal justice. Jurisdictional conflicts emerge because evidence is dispersed across transnational digital infrastructures, while the practical resolution of those conflicts increasingly depends upon private actors that control those infrastructures. The result is a governance structure in which authority over digital evidence is distributed among states, international legal regimes, and multinational technology companies, each exercising different forms of influence over access to information.

This transformation has important implications that extend beyond questions of efficiency and international cooperation. As access to digital evidence becomes increasingly dependent upon complex interactions between public and private actors, significant disparities begin to emerge in the ability of different states to secure and utilize such evidence. The existence of these disparities suggests that the challenges of cross-border digital evidence cannot be understood solely through the lens of jurisdictional conflict or sovereignty. Rather, they raise broader concerns regarding the distribution of evidentiary power within contemporary systems of cybercrime adjudication. It is this issue of unequal access to digital evidence that provides the foundation for the emergence of what this article conceptualizes as the Digital Procedural Divide, a concept examined in the following section.

Unequal Access to Digital Evidence and the Emergence of the Digital Procedural Divide

The use The fragmentation of jurisdiction and the growing privatization of evidentiary access have not affected all states equally. While the challenges associated with cross-border digital evidence are global in scope, the capacity to overcome those challenges is unevenly distributed. States differ significantly in terms of technological infrastructure, legal frameworks, institutional resources, diplomatic influence, and access to transnational cooperation mechanisms. Consequently, the practical ability to obtain, authenticate, and utilize digital evidence increasingly reflects broader asymmetries embedded within the global digital order rather than merely differences in legal authority (Deibert, 2020).

The conventional assumption underlying international criminal cooperation is that states possess relatively comparable capacities to investigate criminal conduct and secure relevant evidence. In practice, however, access to cross-border digital evidence is shaped by profound disparities in investigative capabilities. Advanced economies generally maintain specialized cybercrime units, sophisticated digital forensic laboratories, established cooperation channels with multinational technology companies, and greater participation in international cybercrime governance frameworks (United Nations Office on Drugs and Crime (UNODC), 2024). By contrast, many developing countries continue to face substantial obstacles, including limited digital forensic expertise, inadequate technical infrastructure, resource constraints, and dependence on formal mutual legal assistance procedures that are often slow and ineffective in responding to the speed of digital investigations (United Nations Conference on Trade and Development (UNCTAD), 2024).

These disparities are further exacerbated by the concentration of digital infrastructures within a small number of jurisdictions. A significant proportion of global cloud services, social media platforms, communication applications, and data storage facilities are owned or controlled by corporations headquartered in North America and Western Europe (Kuner, 2013). As a result, states seeking access to digital evidence frequently depend upon legal and institutional arrangements established by a limited number of technologically dominant jurisdictions. The geography of digital infrastructure therefore creates an asymmetrical distribution of evidentiary power in which some states function primarily as providers and regulators of data, while others remain largely dependent consumers of digital evidence.

The problem is not merely one of technological dependency but also of legal and political leverage. Governments with greater geopolitical influence often possess more direct channels of cooperation with major technology companies and are more likely to negotiate bilateral agreements facilitating access to digital evidence. The United States CLOUD Act, for example, allows qualifying foreign governments to enter executive agreements enabling more efficient access to certain categories of data held by U.S.-based service providers (Daskal, 2018b). However, only a limited number of states possess the institutional, legal, and diplomatic capacities necessary to satisfy the requirements for such agreements. Consequently, expedited access mechanisms remain unevenly distributed, creating differentiated levels of evidentiary accessibility across jurisdictions.

The resulting disparities become particularly visible when comparing the pathways through which different states obtain electronic evidence. While some jurisdictions can access subscriber information, metadata, or stored communications through streamlined legal procedures and direct cooperation channels, others remain dependent upon lengthy requests processed through diplomatic and judicial intermediaries. In cybercrime investigations where evidentiary value is often highly time-sensitive, these delays may significantly affect the ability to identify suspects, establish evidentiary chains, or secure successful prosecutions (Council of Europe, 2022). Thus, although states may possess formally equivalent jurisdictional rights, they frequently operate under substantially unequal practical conditions.

The unequal distribution of access to digital evidence can be conceptualized as a form of structural inequality within transnational criminal justice. Existing scholarship has acknowledged disparities in cyber capacity and digital governance; however, these discussions have generally focused on cybersecurity readiness, technological development, or international cooperation (Taylor, 2017). Less attention has been devoted to the procedural consequences of such disparities within criminal adjudication. The present study argues that unequal access to digital evidence

should be understood not merely as an operational challenge but as a systemic feature of contemporary evidentiary governance with direct implications for procedural fairness.

To capture this phenomenon, this article introduces the concept of the Digital Procedural Divide. The concept refers to a structural disparity in the ability of states and litigants to obtain, authenticate, preserve, and utilize cross-border digital evidence in criminal proceedings. Unlike traditional discussions of the digital divide, which focus primarily on disparities in access to information technologies, the Digital Procedural Divide concerns inequalities in access to evidentiary resources necessary for the effective operation of criminal justice systems. It highlights how differences in technological capacity, institutional arrangements, legal frameworks, and geopolitical influence shape the practical realization of procedural rights in cybercrime adjudication.

The emergence of the Digital Procedural Divide may be understood through four interconnected dimensions: technological capacity, legal accessibility, institutional capability, and geopolitical leverage. Together, these dimensions determine the extent to which states and legal actors can effectively participate in contemporary systems of digital evidence governance.

Table 1. Dimensions of the Digital Procedural Divide

Dimension	Characteristics of High-Capacity Jurisdictions	Characteristics of Low-Capacity Jurisdictions
Technological Capacity	Advanced digital forensic infrastructure, cyber investigation units, AI-assisted evidence analysis	Limited forensic facilities, shortage of cybercrime specialists
Legal Accessibility	Direct cooperation mechanisms, executive agreements, efficient evidence disclosure frameworks	Dependence on MLATs and lengthy international requests
Institutional Capability	Specialized prosecutors, trained judges, integrated cybercrime institutions	Fragmented institutional coordination and limited expertise
Geopolitical Leverage	Strong bargaining power with technology companies and foreign governments	Limited influence over transnational service providers
Practical Consequence	Faster acquisition and utilization of digital evidence	Delayed, incomplete, or inaccessible digital evidence

Source: Developed by the author based on synthesis of international cybercrime governance literature.

The significance of this framework lies in its ability to explain why formally equivalent legal rights often produce substantially different procedural outcomes. Under traditional legal reasoning, states exercising criminal jurisdiction are assumed to possess comparable opportunities to collect and present evidence. Yet the reality of contemporary cybercrime investigations suggests otherwise. The effectiveness of evidentiary access increasingly depends upon factors external to formal legal authority, including technological sophistication, institutional resources, and proximity

to centers of digital power (Svantesson, 2017). In this sense, procedural inequality emerges not from the absence of legal rights but from unequal capacities to exercise those rights.

The concept of the Digital Procedural Divide also reveals an important transformation in the nature of inequality within criminal justice systems. Historically, procedural inequalities were often analyzed in terms of disparities between prosecutors and defendants, unequal access to legal representation, or discriminatory application of legal rules. In the digital environment, however, procedural inequality increasingly operates at the transnational level, where disparities among states shape the availability and quality of evidence upon which criminal adjudication depends. This shift reflects the growing influence of global digital infrastructures on the administration of justice and demonstrates that evidentiary power has become a critical component of contemporary legal inequality (Pillsbury, 2019).

Importantly, the Digital Procedural Divide does not imply that all states are permanently disadvantaged or that technological inequalities are insurmountable. Rather, the concept serves as an analytical framework for identifying structural conditions that systematically influence access to digital evidence. By highlighting these conditions, it becomes possible to move beyond narrow debates concerning jurisdiction and sovereignty and toward a broader examination of procedural equality within transnational criminal justice.

The emergence of the Digital Procedural Divide therefore represents a critical development in the evolution of cybercrime adjudication. As criminal investigations become increasingly dependent upon cross-border digital evidence, disparities in evidentiary access are likely to exert growing influence over investigative effectiveness, prosecutorial success, and judicial outcomes. These developments raise fundamental questions regarding the compatibility of contemporary digital evidence governance with established principles of fairness, equality, and due process. Accordingly, the next section examines how the Digital Procedural Divide challenges traditional understandings of procedural equality and contributes to the erosion of equal justice in global cybercrime adjudication.

Digital Procedural Divide and the Erosion of Procedural Equality in Cybercrime Adjudication

The emergence of the Digital Procedural Divide extends beyond questions of investigative efficiency and international cooperation. More fundamentally, it challenges one of the core normative foundations of modern criminal justice systems: procedural equality. Across diverse legal traditions, the legitimacy of criminal adjudication rests upon the assumption that legal processes provide fair and equal opportunities for parties to present evidence, challenge opposing

claims, and participate meaningfully in judicial proceedings (Tyler, 2021). Although absolute equality may never be fully attainable, procedural justice requires that disparities in outcomes arise from the merits of the case rather than from structural inequalities embedded within the adjudicative process itself.

In conventional criminal proceedings, discussions of procedural equality have generally focused on the relationship between defendants and prosecuting authorities. Issues such as access to legal representation, disclosure obligations, evidentiary standards, and judicial impartiality are traditionally regarded as essential safeguards for ensuring fairness in criminal adjudication (Granados, 2024). However, the increasing dependence of criminal investigations on cross-border digital evidence introduces a new dimension of procedural inequality that operates not only between individual parties but also across jurisdictions. The availability of crucial evidence is increasingly shaped by transnational digital infrastructures, platform governance arrangements, and unequal state capacities, factors that often remain outside the control of courts and litigants.

The significance of this transformation becomes apparent when considering the role of evidence within criminal adjudication. Evidence constitutes the foundation upon which judicial determinations of guilt, innocence, and liability are constructed. The ability to obtain relevant evidence is therefore inseparable from the realization of procedural fairness. Where access to evidence is systematically constrained, delayed, or unevenly distributed, the integrity of the adjudicative process itself may be compromised (Damaska, 2017). Consequently, procedural equality cannot be assessed solely by examining formal legal rights; it must also consider the practical conditions under which evidentiary access occurs.

The Digital Procedural Divide exposes a growing disconnect between formal equality and substantive equality within cybercrime adjudication. From a formal legal perspective, states participating in international criminal cooperation frameworks generally possess equivalent rights to request electronic evidence located abroad. Likewise, parties appearing before courts are theoretically entitled to rely upon evidentiary mechanisms recognized by applicable procedural rules. Yet the practical realization of those rights depends heavily upon technological resources, institutional expertise, international cooperation networks, and access to digital infrastructures (Svantesson, 2017). As discussed in the previous section, these capacities are unevenly distributed. Consequently, legal equality at the normative level does not necessarily translate into equality at the operational level.

This phenomenon may be understood through the distinction between procedural equality and procedural capability. Procedural equality refers to the formal recognition of equal legal rights within adjudicative processes, whereas procedural capability concerns the actual ability of legal

actors to exercise those rights effectively. In the context of cross-border digital evidence, procedural capability increasingly depends upon factors external to traditional legal doctrine, including cyber-investigative capacity, digital forensic expertise, and access to transnational information networks (Sen, 2009). The Digital Procedural Divide emerges precisely where disparities in procedural capability undermine the practical effectiveness of formally equal legal rights.

The implications of this divide are particularly significant for the principle of equality of arms, a foundational component of fair trial guarantees recognized in international human rights law. The principle requires that parties in legal proceedings be afforded a reasonable opportunity to present their case without suffering substantial disadvantages relative to opposing parties (Medvedeva et al., 2020). While the doctrine has traditionally been applied within domestic judicial proceedings, its underlying rationale remains relevant to transnational cybercrime adjudication. Where access to critical digital evidence is contingent upon unequal technological and institutional capacities, significant imbalances may arise that affect the ability of parties to investigate facts, challenge allegations, and present effective legal arguments.

Moreover, the Digital Procedural Divide raises concerns regarding access to justice in the digital age. Contemporary scholarship increasingly recognizes that access to justice encompasses more than the formal availability of legal remedies; it also includes the practical ability to utilize legal institutions effectively (Lotysh & Balatska, 2024). In cybercrime cases, the inability to obtain or verify relevant digital evidence may prevent victims from securing legal redress, impede prosecutors from establishing criminal responsibility, or restrict defendants from challenging incriminating allegations. Thus, unequal evidentiary access may affect multiple actors within the justice system, generating broader concerns regarding the fairness and legitimacy of judicial outcomes.

These concerns become even more pronounced when viewed through the lens of digital constitutionalism. Emerging scholarship on digital constitutionalism argues that the exercise of power within digital environments must remain subject to principles of accountability, transparency, fairness, and rights protection (Celeste, 2022). Although much of this literature focuses on platform governance and online expression, its normative insights are equally relevant to the governance of digital evidence. If access to evidence increasingly depends upon decisions made by private technology companies, opaque disclosure policies, and asymmetrical technological capacities, then fundamental procedural guarantees risk becoming contingent upon factors external to democratic legal institutions. Such a development challenges traditional assumptions regarding the rule of law and the equal administration of justice.

The erosion of procedural equality is not merely a theoretical concern. In practical terms, disparities in evidentiary access may influence every stage of the adjudicative process. Delays in obtaining data may hinder investigations, incomplete disclosures may affect prosecutorial decision-making, and difficulties in authenticating digital evidence may weaken judicial confidence in evidentiary reliability. These effects are particularly acute in cybercrime cases, where digital traces frequently constitute the primary or even sole source of relevant evidence (Kerr, 2022). Consequently, unequal access to electronic evidence can have direct implications for the accuracy, fairness, and legitimacy of criminal adjudication.

To clarify the relationship between the Digital Procedural Divide and procedural equality, the following table summarizes the principal procedural consequences associated with unequal access to cross-border digital evidence.

Table 2. The Impact of the Digital Procedural Divide on Procedural Equality

Principle of Procedural Justice	Impact of the Digital Procedural Divide	Potential Consequence
Equality Before the Law	Unequal evidentiary capabilities among jurisdictions	Inconsistent enforcement outcomes
Equality of Arms	Asymmetrical access to digital evidence	Imbalance between parties in litigation
Due Process	Delays and obstacles in obtaining relevant evidence	Reduced procedural fairness
Access to Justice	Limited ability to secure or challenge digital evidence	Restricted legal remedies
Fair Trial	Dependence on incomplete or inaccessible evidence	Increased risk of erroneous outcomes

Source: Developed by the author based on the synthesis of procedural justice, cybercrime governance, and digital evidence literature.

The analysis above demonstrates that the Digital Procedural Divide should not be viewed merely as a technical challenge associated with cybercrime investigations. Rather, it constitutes a structural condition that reshapes the distribution of procedural opportunities within contemporary systems of criminal justice. By influencing who can access evidence, under what conditions, and with what degree of effectiveness, the divide affects the practical realization of fundamental principles that underpin the legitimacy of adjudicative institutions.

Accordingly, the challenge posed by cross-border digital evidence is no longer confined to questions of jurisdictional authority or investigative efficiency. It has evolved into a broader issue of procedural justice within a digitally interconnected world. Addressing this challenge therefore requires more than incremental improvements to existing cooperation mechanisms. It necessitates a rethinking of how digital evidence is governed and distributed within transnational legal systems to ensure that technological transformation does not undermine the foundational commitment of

criminal justice to equality, fairness, and the rule of law. This imperative forms the basis for the development of a more equitable framework of global digital evidence governance, discussed in the following section.

Toward an Equitable Framework for Global Digital Evidence Governance

The preceding discussion demonstrates that the challenges surrounding cross-border digital evidence cannot be resolved solely through the expansion of jurisdictional authority or the acceleration of international cooperation mechanisms. While initiatives such as the Budapest Convention, the CLOUD Act, and the European Union's E-Evidence Regulation have undoubtedly improved the efficiency of transnational evidence gathering, they have largely been designed to address problems of access and enforcement rather than the broader issue of procedural equality. Consequently, contemporary reforms risk reproducing existing asymmetries if they focus exclusively on facilitating evidentiary access without addressing the structural disparities that shape who can effectively exercise such access (Daskal, 2018b).

The emergence of the Digital Procedural Divide suggests that the governance of cross-border digital evidence should be reconceptualized as a question of procedural justice rather than merely a matter of investigative efficiency. Existing legal frameworks are primarily concerned with enabling access to digital evidence across jurisdictions, yet they devote considerably less attention to the unequal distribution of technological, institutional, and legal capacities among states. As a result, reforms intended to improve cooperation may inadvertently benefit jurisdictions that already possess advanced cyber-investigative capabilities while leaving existing disparities largely intact (United Nations Office on Drugs and Crime (UNODC), 2024).

Addressing this challenge requires a shift from an access-oriented model of digital evidence governance toward an equity-oriented model. Under an access-oriented approach, success is measured by the ability of authorities to obtain electronic evidence more rapidly and efficiently. By contrast, an equity-oriented approach evaluates whether legal frameworks provide meaningful and relatively equal opportunities for different jurisdictions and legal actors to obtain, preserve, authenticate, and utilize digital evidence within criminal proceedings. Such an approach recognizes that procedural fairness depends not only on the existence of legal rights but also on the practical conditions necessary to exercise those rights effectively (Sen, 2009).

An equitable framework for global digital evidence governance should therefore be guided by four interrelated normative principles:

The first principle is procedural equality. Access to digital evidence should not be determined primarily by a state's geopolitical influence, technological sophistication, or bargaining power with multinational technology companies. Instead, international cooperation mechanisms should seek

to minimize disparities that systematically disadvantage certain jurisdictions in obtaining relevant evidence. This principle does not require identical outcomes for all states; rather, it requires the establishment of legal and institutional arrangements that reduce unjustified asymmetries in evidentiary access (Rawls, 1971).

The second principle is transparency and accountability in platform-mediated evidence governance. As discussed earlier, private technology companies increasingly function as gatekeepers of digital evidence. Their internal policies regarding data retention, disclosure procedures, transparency reporting, and responses to governmental requests have significant implications for criminal investigations and judicial proceedings. Yet many of these practices remain governed by private decision-making processes that are only partially visible to public authorities and judicial institutions. An equitable governance framework therefore requires greater transparency regarding how evidentiary decisions are made and stronger accountability mechanisms to ensure consistency, fairness, and respect for fundamental rights (Cohen, 2019; Suzor, 2019).

The third principle is capacity-sensitive international cooperation. Contemporary systems of cybercrime governance often assume that participating states possess comparable institutional capabilities. In reality, however, significant disparities exist in digital forensic expertise, technological infrastructure, financial resources, and legal specialization. Effective international cooperation should therefore incorporate mechanisms designed to strengthen the capacities of states facing structural disadvantages in accessing digital evidence. Such measures may include technical assistance programs, specialized training initiatives, digital forensic support networks, and the development of shared investigative resources (United Nations Office on Drugs and Crime (UNODC), 2024). By addressing underlying capacity gaps, international cooperation can contribute not only to more effective enforcement but also to greater procedural equality.

The fourth principle is human rights-based digital evidence governance. The collection and use of electronic evidence inevitably implicate a range of fundamental rights, including privacy, due process, fair trial guarantees, and access to justice. Consequently, reforms aimed at improving evidentiary access should be evaluated not solely according to their effectiveness in facilitating investigations but also according to their compatibility with broader human rights standards. A governance framework that prioritizes efficiency at the expense of procedural safeguards may ultimately undermine the legitimacy of criminal adjudication (Celeste, 2022). Conversely, integrating human rights principles into digital evidence governance can help ensure that efforts to combat cybercrime remain consistent with the rule of law and democratic accountability.

Taken together, these principles provide the foundation for a more balanced approach to cross-border digital evidence governance. Rather than treating efficiency and fairness as competing objectives, the proposed framework recognizes that sustainable and legitimate systems of digital evidence governance must pursue both simultaneously. Effective cybercrime enforcement cannot be achieved if large segments of the international community remain structurally disadvantaged in accessing evidence. Likewise, procedural equality cannot be realized if legal frameworks fail to account for the technological realities of contemporary digital investigations.

The concept of the Digital Procedural Divide contributes to this reconceptualization by highlighting the relationship between evidentiary access and procedural justice. Existing debates have largely framed cross-border digital evidence as a problem of sovereignty, jurisdiction, or international cooperation. While these concerns remain important, they do not fully capture the distributive dimensions of evidentiary governance in the digital age. The Digital Procedural Divide reveals that access to evidence has become a critical site through which power, capability, and inequality are reproduced within transnational criminal justice systems. Recognizing this reality enables a more comprehensive understanding of the challenges confronting contemporary cybercrime adjudication.

Ultimately, the future of global digital evidence governance will depend on the ability of legal systems to reconcile technological transformation with foundational principles of justice. As digital infrastructures continue to transcend territorial boundaries, the legitimacy of criminal adjudication will increasingly be measured not only by the effectiveness of investigative powers but also by the fairness with which access to evidence is distributed across jurisdictions. From this perspective, reducing the Digital Procedural Divide is not merely a technical objective of cybercrime regulation; it is a normative imperative for preserving procedural equality and ensuring equal access to justice in an increasingly interconnected digital world.

Conclusion

This article has demonstrated that the challenges surrounding cross-border digital evidence cannot be adequately understood through conventional debates on jurisdiction, sovereignty, or international cooperation alone. The increasing dependence of cybercrime investigations on data controlled by transnational digital infrastructures has transformed access to evidence into a critical issue of procedural justice. While existing legal frameworks seek to facilitate the collection of electronic evidence across borders, they operate within a global digital environment characterized by significant disparities in technological capacity, institutional resources, and access to platform-controlled information.

The principal contribution of this study is the development of the concept of the Digital Procedural Divide, defined as a structural disparity in the ability of states and legal actors to obtain, authenticate, and utilize cross-border digital evidence in criminal proceedings. The analysis demonstrates that unequal access to digital evidence creates a gap between formal legal rights and practical procedural capabilities, thereby undermining fundamental principles of equality before the law, due process, equality of arms, and access to justice in cybercrime adjudication.

These findings suggest that the governance of digital evidence should be reconceptualized as a matter of procedural equality rather than merely investigative efficiency. Accordingly, efforts to reform cross-border digital evidence regimes should move beyond expanding evidentiary access and address the structural inequalities that shape the distribution of evidentiary power in the digital age. An equitable framework for global digital evidence governance must therefore incorporate principles of procedural equality, platform accountability, capacity-sensitive international cooperation, and human rights protection.

Ultimately, as criminal justice systems become increasingly dependent on transnational digital infrastructures, the legitimacy of cybercrime adjudication will depend not only on the effectiveness of investigative mechanisms but also on the fairness with which access to digital evidence is distributed. Reducing the Digital Procedural Divide is therefore essential to ensuring that technological transformation strengthens, rather than undermines, the fundamental values of justice and the rule of law in the digital era.

References

- Abraha, H. H. (2020). Regulating law enforcement access to electronic evidence across borders: the United States approach. *Information and Communications Technology Law*. <https://doi.org/10.1080/13600834.2020.1794617>
- Balkin, J. M. (2018). Free speech is a triangle. In *Columbia Law Review* (Vol. 118, Issue 7).
- Celeste, E. (2022). *Digital constitutionalism: The role of internet bills of rights*. Routledge. <https://doi.org/10.4324/9781003256908>
- Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.
- Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*. Council of Europe Publishing.
- Damaska, M. R. (2017). *Evidence Law Adrift*. Yale University Press. <https://doi.org/10.12987/9780300146479>
- Daskal, J. (2018a). Borders and bits. *Vanderbilt Law Review*, 71(1).
- Daskal, J. (2018b). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Stanford*

- Deibert, R. J. (2020). Reset: Reclaiming the Internet. *Social Media in Society*, 11(3).
- European Commission. (2018). *Impact Assessment Report Accompanying the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*. European Commission.
- Granados, J. S. A. P. (2024). The criminal process mediated by artificial intelligence. *Revista Brasileira de Direito Processual Penal*, 10(2). <https://doi.org/10.22197/rbdpp.v10i2.988>
- Gutwirth, S., & De Hert, P. (2022). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. *Direito Público*, 18(100). <https://doi.org/10.11117/rdp.v18i100.6200>
- Hutchinson, T. (2024). *Researching and Writing in Law* (4th ed.). Lawbook Co.
- Hutchinson, T., & Duncan, N. (2012). Defining and Describing What We Do: Doctrinal Legal Research. *Deakin Law Review*, 17(1). <https://doi.org/10.21153/dlr2012vol17no1art70>
- Kerr, O. S. (2022). *Computer Crime Law* (5th ed.). West Academic Publishing.
- Kuczyńska, H. (2024). The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change. *Studia Iuridica Lublinensia*, 33(5). <https://doi.org/10.17951/sil.2024.33.5.125-153>
- Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>
- Lotysh, T., & Balatska, O. (2024). The right to effective access to justice in the European Union. *Visegrad Journal on Human Rights*, 4. <https://doi.org/10.61345/1339-7915.2024.4.2>
- Medvedeva, M., Vols, M., & Wieling, M. (2020). Using machine learning to predict decisions of the European Court of Human Rights. *Artificial Intelligence and Law*, 28(2). <https://doi.org/10.1007/s10506-019-09255-y>
- Moise, A. C. (2024). Procedural Aspects of the Second Additional Protocol to the Council of Europe Convention on Cybercrime. *Bulletin of the Transilvania University of Braşov. Series VII: Social Sciences • Law*. <https://doi.org/10.31926/but.ssl.2023.16.65.3.23>
- Pillsbury, S. H. (2019). Victims and Justice under Law. In *Imagining a Greater Justice*. <https://doi.org/10.4324/9780429424922-11>
- Radoniewicz, F. (2025). Cybercrime in the law of the Council of Europe (part I) – Convention on Cybercrime. In *Cybercrime and the Law*. <https://doi.org/10.4324/9781003476771-3>
- Rawls, J. (1971). *A Theory of Justice*. Harvard University Press, Belknap Press. <https://doi.org/https://doi.org/10.2307/j.ctvjf9z6v>
- Ryngaert, C. (2025). The concept of jurisdiction in international law. In *Research Handbook on Jurisdiction and Immunities in International Law, Second Edition*. <https://doi.org/10.4337/9781035331086.00007>

- Sachoulidou, A. (2024). 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*, 15(3). <https://doi.org/10.1177/20322844241258649>
- Sen, A. (2009). *The Idea of Justice*. Harvard University Press.
- Suzor, N. P. (2019). *Lawless the secret rules that govern our digital lives*. Cambridge University Press. <https://doi.org/10.1017/9781108666428>
- Svantesson, D. J. B. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford University Press. <https://doi.org/10.1093/oso/9780198795674.001.0001>
- Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data and Society*, 4(2). <https://doi.org/10.1177/2053951717736335>
- Tyler, T. R. (2021). *Why People Obey the Law* (3rd ed.). Princeton University Press. <https://doi.org/10.2307/j.ctv1j66769>
- United Nations Conference on Trade and Development (UNCTAD). (2024). *Digital Economy Report 2024: Shaping an Inclusive Digital Future*. United Nations.
- United Nations Office on Drugs and Crime (UNODC). (2024). *Comprehensive Study on Cybercrime*. United Nations.
- Zumbansen, P. (2012). Transnational law, evolving. In *Elgar Encyclopedia of Comparative Law, Second Edition*. <https://doi.org/10.4337/9781781006108.00078>