INTEGRATED LEGAL ENFORCEMENT CHALLENGES REGARDING CROSS-BORDER DIGITAL FRAUD AND ITS IMPLICATIONS FOR REGULATORY REFORM

Ahmad Wahyudi, Pratolo Saktiawan, Rio Saputra, Sarwo Waskito, Kurnia Wijaya

Universitas Sunan Giri Surabaya

Correspondence: dr.riosaputra@gmail.com

ABSTRACT

The phenomenon of cross-border digital fraud poses substantial challenges for national legal systems still dominated by territorial principles. The existence of offenders operating from abroad, gaps in legislative frameworks, and a lack of synergy among institutions create significant barriers to law enforcement and restitution. This study analyzes the adequacy of existing statutory instruments and the international cooperation mechanisms that have been implemented, highlighting various regulatory limitations, obstacles to institutional coordination, and technological adaptation gaps in law enforcement processes. Conversely, comparative analyses with advanced legal systems demonstrate the critical relevance of harmonization with international conventions, the governance of centralized cyber authorities, and the enhancement of technical capacities as key factors in expediting cross-jurisdictional coordination. Active engagement in multilateral digital efforts, accession to cybercrime agreements, and the strengthening of reporting and asset recovery systems are identified as cornerstones for achieving legal protection in the digital era. Reforms centered on the establishment of cross-sectoral national institutions, advancing cyber human resource quality, and developing forensic and asset tracing technologies are expected to improve the efficacy of combating digital crime across borders. This research recommends the strengthening of coordination, harmonization of national legal frameworks with global standards, and procedural innovations to support speed and accuracy of response. The findings affirm that optimal efforts to develop a responsive and adaptive cross-border digital fraud mitigation system constitute a pivotal step towards fostering a more secure and trustworthy digital ecosystem.

Keywords: digital fraud, jurisdiction, international cooperation, cybercrime, cross-border assets, legal reform, cyber authority.

INTRODUCTION

In recent decades, the global expansion of digital technology has revolutionized commerce, communication, and various forms of social interaction while simultaneously enabling a new wave of illicit activities that are no longer constrained by physical borders. Digital fraud, especially those committed by actors operating beyond national frontiers, has emerged as one of the most pressing legal concerns confronting states. This transnational challenge disrupts established paradigms of law enforcement and governance, necessitating innovative responses

both domestically and internationally. Within this new paradigm, nations find themselves compelled to confront cybercriminals employing sophisticated methods to exploit legal and procedural gaps across multiple jurisdictions (Amoo et al., 2024).

In the Indonesian legal landscape, cross-border digital fraud has been particularly problematic due to the complexity of pursuing perpetrators residing outside territorial boundaries. The globalization of communication networks, proliferation of online platforms, and the advent of cryptocurrencies have exacerbated these problems. Indonesian authorities frequently encounter substantial hurdles when investigating, prosecuting, and executing judgments against offenders who cloak their identities, exploit technical loopholes, and leverage international safe havens. Furthermore, such digital misconduct often involves stolen identities, manipulation of e-commerce platforms, and extensive use of encrypted communication protocols that hinder detection and enforcement (Fajria & Ilmih, 2024).

A core issue lies in the jurisdictional limitations of the Indonesian legal system when addressing crimes committed in the digital domain. Traditional concepts of territorial sovereignty are increasingly undermined by actors who transcend national boundaries and operate from distant locations. The significant distance between the locus of crime and the location of the perpetrator, compounded by differing national legal frameworks, presents formidable challenges for investigators and prosecutors alike. As a result, efforts to hold offenders accountable become diluted, often leading to impunity for those most adept at exploiting the gaps between national laws (Martono et al., 2025; Yu et al., 2024).

Indonesian regulatory responses have developed through several important legislative instruments, including the amended Law No. 1 of 2024 on Electronic Information and Transactions and Law No. 27 of 2022 concerning Personal Data Protection (Panjaitan et al., 2024; Anggriawan & Susila, 2024). Nevertheless, these frameworks largely operate within a domestic scope and remain insufficiently aligned with established international legal instruments. Mechanisms such as mutual legal assistance treaties (MLA) and extradition are present but frequently encounter obstacles due to a lack of bilateral agreements, divergent legal definitions, or limited recognition of digital fraud as a serious offense in some countries (Wong, 2024). The absence of a specialized, cross-sectoral body managing international digital fraud renders responses fragmented, undermining the national capacity to respond effectively.

In addition, major substantive and procedural hurdles complicate law enforcement. Complexities arise when attempting to secure digital evidence scattered across several countries, as different legal standards and political considerations come into play (Sudarwanto & Kharisma, 2023). The lack of harmonization between domestic statutes and global initiatives, coupled with scarce technical capabilities and delays in international cooperation, exacerbates the prevailing enforcement gap. Indonesia's struggle to protect its citizens and economic infrastructure underscores the pressing need for reform and a systematic, internationally coordinated legal response (Maksum, 2024).

The centrality of jurisdictional uncertainty, technical barriers, and the weakness of intergovernmental coordination frame this study's concern. Most notably, the globalized nature of digital fraud is such that state-centric approaches fail to offer comprehensive recourse. To adequately address threats that emerge from technological advancements and the rapid

globalization of criminal modalities, Indonesian authorities must pursue expanded legal, regulatory, and institutional capacities that are adaptive, resilient, and informed by comparative global experiences. This normative juridical study thereby probes the sufficiency and coherence of Indonesian legal instruments confronting transnational digital fraud and underscores the importance of harmonizing domestic regulations with international cooperation.

A predominant concern stems from the pronounced jurisdictional fragmentation in pursuing digital fraudsters located abroad. As noted by Martono et al. (2025), enforcement agencies are confronted not just with conflicting national jurisdictions, but also with the absence of procedural harmony required to coordinate investigations, facilitate asset recovery, and effect extradition. This mismatch leads to significant enforcement gaps, with offenders often avoiding prosecution by exploiting safe jurisdictions with weak law enforcement, inconsistent legal classifications, or the absence of extradition frameworks tailored to cybercrime. Consequently, Indonesian victims of digital fraud suffer from inaccessible remedies and prolonged periods of legal uncertainty.

Equally significant is the procedural inadequacy within Indonesia's mutual legal assistance and extradition arrangements (Yu et al., 2024; Wong, 2024). Many transnational cooperation requests suffer from protracted bureaucratic processes and political delays. Several countries in Southeast Asia lack comprehensive bilateral agreements or have limited engagement with global conventions such as the Budapest Convention, further restricting the capacity for evidence sharing and collaborative prosecutions. According to Anggriawan and Susila (2024), this legal disconnect is particularly detrimental given the technical sophistication of digital fraud, which demands swift and well-coordinated responses to preserve evidence, secure suspects, and prevent financial assets from dissipating across borders.

Beyond jurisdictional and procedural limitations, Indonesia's institutional infrastructure remains insufficiently integrated (Panjaitan et al., 2024; Maksum, 2024). Fragmented responses among law enforcement bodies, regulatory authorities, and financial intelligence units create strategic vulnerabilities. The absence of a centralized coordination agency, as recommended by comparative studies (Sudarwanto & Kharisma, 2023), leads to inefficient case management and underutilization of existing legal tools. As a result, transnational digital fraud cases are often delayed or remain unresolved, revealing systematic challenges in Indonesia's current legal and institutional response.

There is considerable necessity to observe and analyze these matters for several important reasons. The unchecked proliferation of cross-border digital fraud has grave implications for public trust in digital financial systems and the overall security of society. With cybercriminals targeting a range of digital platforms, from online banking to e-commerce, the resulting economic and social costs have been substantial and require urgent legal attention. Moreover, the failure to effectively respond undermines Indonesia's credibility and deterrence capability in the international community, risking reputational damage and potential diplomatic disputes.

The adequacy of the existing Indonesian legal philosophy and mechanisms to address these transnational crimes will define the future resilience of national and private entities within the digital sphere. By examining the gaps between current laws, institutional frameworks, and best practices from other jurisdictions, this analysis provides critical insight into the strategic directions necessary for enhancing sovereign legal authority and fortifying the protection of society against complex digital threats. A literature-based juridical synthesis remains indispensable for mapping the evolving interplay between domestic and international legal systems in this domain.

This study aims to critically evaluate the adequacy of jurisdictional arrangements and international cooperation strategies employed by Indonesia in combatting cross-border digital fraud. It further seeks to elucidate the strengths and limitations of existing legislative instruments and institutional mechanisms in responding to cases with international dimensions. The outcomes of this study are expected to contribute an original, nuanced understanding of Indonesia's standing within global cybercrime governance and offer empirically grounded recommendations to enhance legal reform, state capacity, and international collaboration.

RESEARCH METHODS

This study applies a qualitative literature-based approach, placing emphasis on document analysis and thematic synthesis to explore the adequacy of Indonesia's legal instruments and institutional frameworks in addressing cross-border digital fraud. Drawing from established methods in socio-legal research, the investigation systematically reviews peer-reviewed journal articles, statutory regulations, and authoritative reports to identify thematic patterns, comparative practices, and conceptual gaps in the enforcement of transnational digital fraud laws. Flick (2018) underlines the necessity of utilizing a comprehensive literature analysis for understanding the complexity of social phenomena, particularly when empirical access is limited due to the covert nature of cybercrime.

The method entails critical selection and in-depth examination of secondary data, encompassing both Indonesian and international legal sources. This includes an extensive review of statutes, regulatory guidelines, and scholarly discourse related to mutual legal assistance, extradition, digital evidence, and legislative adaptation to technological evolution. As explained by Creswell and Poth (2018), qualitative document analysis permits the scholar to extract nuanced insights, enabling the identification of recurring themes and the evaluation of causative factors underlying enforcement gaps. Thematic synthesis is then employed to integrate findings from diverse materials into a coherent analytical framework.

Furthermore, triangulation is pursued by cross-referencing the findings against diverse jurisdictions and legal scholarship to enhance validity and reliability. Stake (2010) recommends triangulation as a means of counteracting methodological bias and fostering a more balanced assessment of normative arguments, procedural inefficacies, and institutional responses. Through this qualitative and document-centric approach, the research aims to generate substantive knowledge about the interplay between national regulation, international legal cooperation, and practical enforcement in the fight against cross-border digital fraud.

RESULTS AND DISCUSSION

Jurisdictional and International Cooperation Gaps

The rapid evolution of communication technologies has fundamentally transformed the landscape of criminal activity, giving rise to new forms of digital offenses that transcend traditional geographical boundaries. These technological advancements have enabled perpetrators to operate seamlessly across jurisdictions, leveraging the internet's borderless nature to perpetrate complex schemes with limited risk of immediate detection or intervention by national authorities (Sousa, 2023). As a result, states are increasingly confronted with legal and practical dilemmas in their pursuit of justice, as local laws—crafted within the confines of national borders—struggle to keep pace with crimes that unfold in virtual, multi-jurisdictional arenas (Kazandjiski, 2015). This reality necessitates a critical reexamination of how legal systems define, detect, and respond to digital wrongdoing in an era where transnational criminal operations have become the norm rather than the exception.

The sufficiency of existing jurisdictional frameworks and international cooperation mechanisms in addressing law enforcement against cross-border digital fraud remains highly contested (Kumar, 2024). The prevailing legal order in Indonesia, as in many developing countries, is primarily anchored to the principle of territoriality. This approach, while central to classical criminal law enforcement, is increasingly incongruent with the transnational character of digital crime, especially when the perpetrators operate beyond state boundaries (Asghar et al., 2025). Digital fraudsters exploit anonymity, jurisdictional fragmentation, and technical prowess by deploying operations that straddle multiple national regimes, making identification, pursuit, and prosecution profoundly complicated.

The prevailing jurisdictional paradigm still widely adopts approaches rooted in physical sovereignty, resulting in conflicting interpretations and practical obstacles. National laws, such as Indonesia's Law No. 1 of 2024 on Electronic Information and Transactions and Law No. 27 of 2022 on Personal Data Protection, provide formal authority over cyber-related offenses but remain largely domestically oriented and are not fully harmonized with international norms (Ali et al., 2024). This misalignment restricts Indonesia's capability to streamline investigative efforts or to facilitate international legal support expediently, especially when evidence collection, forensic tracing, and suspect apprehension require extensive cross-border cooperation. As a result, enforcement agencies often face protracted delays and procedural barriers, undermining the overall effectiveness of cybercrime deterrence measures. Furthermore, the lack of a unified legal framework can create safe havens for perpetrators who exploit jurisdictional loopholes and disparities in national enforcement priorities. Strengthening Indonesia's position in combating cyber-related offenses therefore necessitates comprehensive alignment of domestic regulations with global standards and intensified participation in multilateral cybercrime initiatives. Only through such legal harmonization and collaborative engagement can the complexities of transnational cyber threats be addressed with the requisite agility and efficacy.

The problem is further aggravated by divergent definitions of cybercrime, inconsistent procedural requirements, and a generally low rate of accession to multilateral conventions such as the Budapest Convention on Cybercrime. As observed by Buçaj and Idrizaj (2025), despite

its status as a global reference standard, Indonesia is yet to become a party, resulting in significant limitations surrounding mutual legal assistance, evidence sharing, and extradition. Consequently, suspects frequently evade justice by exploiting safe jurisdictions or countries unwilling or unable to cooperate, thereby perpetuating the impunity gap across digital-transnational fraud cases.

International cooperation under mechanisms like mutual legal assistance treaties (MLA) and extradition agreements is often slow, administratively cumbersome, and hampered by the lack of uniformly applicable definitions or procedural congruity. Reports by Wong (2024) and Yu, Cong, and Li (2024) demonstrate that requests for evidence or suspect extradition are often delayed or even denied, particularly when the requested country does not recognize digital fraud as a predicate crime, or when bilateral relations are weak. This vulnerability is acutely felt in fast-moving or technically complex cases, where delay equates to the dissipation of the digital trail or asset flight to further jurisdictions.

Despite the shortcomings, there are traces of incremental development in international practice—for example, the emergence of ad hoc regional collaborations (such as in ASEAN or INTERPOL), diplomatic protocols, and the use of Joint Investigative Teams. Such measures, while promising, remain sporadic and highly dependent on voluntary engagement rather than binding obligations. Peters and Jordan (2019) argue that the lack of binding global rules leaves most law enforcement agencies reliant on goodwill, causing sporadic efficacy and undermining the deterrence effect on transnational criminals.

On a practical level, the complexity of digital fraud investigations exacerbates national capacity constraints. Indonesian law enforcement agencies commonly cite difficulties in accessing encrypted data, tracking cryptocurrency transactions, or securing testimony from foreign witnesses (Aryadi et al., 2024). In numerous instances, the evidentiary process becomes protracted or futile because certain jurisdictions lack legislation mandating data preservation or do not impose obligations on service providers domiciled within their borders. This digital evidence vacuum is one of the most acute technical and legal limitations, as highlighted by Aziz et al. (2023) in the context of the fintech sector.

Institutionally, Indonesia's law enforcement is hindered by a fragmented command structure involving agencies such as the police, the Ministry of Communication and Information, and independent regulatory authorities, all without a centralizing national coordinator (Ashurov, 2024). This fragmentation impedes expeditious case handling, reduces accountability, and often dilutes the impact of international cooperation efforts, particularly when rapid action or unified representation are required for engagement with foreign counterparts.

The challenges of asset recovery and enforcement loom large. Funds obtained from digital fraud are rapidly laundered through international financial networks, digital wallets, or cryptocurrencies, creating intricate trails that span several jurisdictions with differing anti-money laundering standards. Rusianto et al. (2023) describe how such proceeds are routinely located offshore, limiting domestic seizure efforts and complicating efforts to secure victim restitution. Divergent legal regimes for recognizing and enforcing asset confiscation requests further erode the practical effectiveness of Indonesia's national frameworks.

Managerially, insufficient and slow adaptation to technological sophistication by law enforcement is a palpable risk. Aryadi et al. (2024) suggest that without continuous professional development and international collaboration, national authorities are left on the backfoot, lacking operational agility against well-resourced cybercriminal networks employing state-of-the-art methods. Cross-border capacity-building programs, joint task forces, and technical knowledge transfer have occurred but remain the exception rather than the standard.

From a theoretical perspective, the enduring dominance of state-centric sovereignty is fundamentally ill-suited to the realities of the digital age. The international legal system's inability to reconcile the gap between physical and virtual criminal conduct allows transnational offenders to exploit the very architecture of international law, using jurisdictional gaps as shields against accountability. As articulated by Buçaj and Idrizaj (2025), only when national frameworks are buttressed by robust multilateral legal commitments can an effective remedial pathway be sustained.

Despite varied efforts, it remains apparent that Indonesia's jurisdictional and international cooperation frameworks, while evolving, have yet to reach a level of sufficiency compatible with the complexities of cross-border digital fraud. Ongoing challenges center on slow procedural exchange, legal incongruence, and insufficient central coordination, compounded by technical and evidentiary deficits. This persistent deficit undermines not only the effectiveness of enforcement but also public confidence in digital ecosystems. The resulting lack of swift and coordinated responses hinders the capacity of authorities to intercept and prosecute cybercriminals operating across multiple jurisdictions. Furthermore, disparate legal interpretations between Indonesia and its international counterparts often delay or inhibit the execution of mutual legal assistance requests, creating loopholes that can be easily exploited by transnational offenders. Without enhanced technical integration and comprehensive capacity-building among law enforcement and judicial actors, procedural inefficiencies will continue to impede progress. Establishing standardized protocols for evidence gathering and information sharing would substantively improve operational consistency and outcome predictability in cross-border cases. Ultimately, addressing these multidimensional shortcomings is essential not only for safeguarding digital transaction integrity, but also for strengthening Indonesia's position within the global fight against digital fraud.

At the heart of the matter, therefore, is an urgent need for Indonesia to expand its diplomatic engagements, accede to relevant international conventions, enhance its domestic statutes, and empower a coordinating institution with a cross-sectoral mandate on digital crime. Without such structural recalibration, law enforcement against transnational digital fraud will remain reactive, fragmented, and inadequate to contemporary exigencies.

National Legal Frameworks and Institutional Adequacy

Efforts to adapt Indonesian law to address the procedural and structural complexities of transnational digital fraud have produced a patchwork of legislative and institutional responses. The primary legislative measures, particularly the amended Law No. 1 of 2024 concerning Electronic Information and Transactions and Law No. 27 of 2022 concerning Personal Data Protection, serve as foundational instruments to criminalize a wide range of digital misconducts and stipulate mechanisms for digital evidence preservation and disclosure (Ali et al., 2024).

Despite this progress, these statutes largely function within a national framework, lacking full harmonization with global conventions, and therefore only partially address the idiosyncrasies of cross-border cases. As a direct consequence, Indonesian authorities frequently encounter significant obstacles in coordinating with foreign law enforcement agencies, which limits the efficiency of joint investigations and mutual legal assistance. Moreover, the absence of universally recognized protocols often results in protracted legal processes and inconsistencies in the treatment of transnational offenders. Such limitations undercut the deterrent effect of domestic regulations and could inadvertently encourage perpetrators to exploit jurisdictional gaps. Addressing these deficiencies requires the systematic integration of international legal standards and the establishment of formal cooperative mechanisms with global partners. Reinforcing Indonesia's legal framework with robust cross-border collaboration and regulatory convergence is thus indispensable for effectively combating the evolving threats posed by transnational digital fraud.

Procedurally, the absence of detailed guidelines for executing cross-jurisdictional investigations and preserving the integrity of electronic evidence remains an obstacle. As elaborated by Baraja et al. (2023), collecting and verifying digital evidence across multiple countries often depends not on clear statutory instruction, but on ad hoc collaboration or goodwill. The technical sophistication of cyber-enabled fraud, particularly when utilizing encrypted channels and decentralized crypto-assets, further complicates the chain of custody and promptness of response. The necessity for expedited cooperation, as practiced under international best standards, is weakened by these statutory gaps.

Institutional fragmentation significantly tempers the effectiveness of existing tools. Multiple authorities—including national police, the Ministry of Communication and Information, the Financial Services Authority (OJK), and Bank Indonesia—share partial responsibility, leading to duplication, delays, and jurisdictional disputes (Ashurov, 2024). Notably absent is a cross-sectoral central body with unified oversight, which impedes case coordination and rapid response to international requests or intelligence. This phenomenon is not unique to Indonesia, but comparative studies reveal that jurisdictions with specialized cyber agencies or task forces record more effective prosecutions and asset recoveries (Sudarwanto & Kharisma, 2023).

Limitations in mutual legal assistance (MLA) and extradition frameworks further curtail Indonesia's reach in pursuing digital fraudsters abroad (Panjaitan et al., 2024; Wong, 2024). Law No. 1 of 2006 on Mutual Legal Assistance offers structural provisions, but practical barriers such as lags in execution, non-uniform digital crime definitions, and varying thresholds for evidence recognition restrict its effectiveness. For example, requests for international assistance often grapple with incompatible standards for electronic proof and reciprocal obligations, diminishing the prospects for timely arrests or asset seizures (Yu et al., 2024).

The evolving threat landscape introduces new forms of crime that outpace regulatory reform. Crypto-based fraud, deepfakes, unauthorized digital asset transfers, and sophisticated phishing strategies necessitate not only legal adaptability but also advanced technical capacities and inter-agency integration (Aryadi et al., 2024; Aziz et al., 2023). Institutional inertia and limited cyber-forensic expertise hinder the translation of statutory commands into actionable intelligence and prosecution. The persistent emergence of technologically complex schemes

demands synchronized policy responses that integrate legislative agility with continual investments in digital forensic infrastructure. Furthermore, the increasing reliance of criminals on anonymizing technologies and decentralized platforms exacerbates the challenges of attribution, evidence preservation, and cross-jurisdictional cooperation, thereby necessitating robust multi-stakeholder collaboration across both public and private sectors. Without comprehensive frameworks for capacity-building and knowledge transfer, law enforcement agencies remain at a strategic disadvantage against cybercriminals who rapidly adapt to new regulatory environments. Ultimately, a paradigm shift is required—one that transcends traditional regulatory boundaries and emphasizes the co-evolution of law, technology, and organizational structures to ensure responsiveness, resilience, and accountability in the fight against digital crime.

The reluctance or slow progress towards adopting global instruments, especially the Budapest Convention on Cybercrime, underscores both sovereignty sensitivities and a lack of readiness (Buçaj & Idrizaj, 2025; Asghar, Javed, & Azhar, 2025). Full participation in such conventions could enhance Indonesia's access to real-time intelligence, accelerate case transfers, and synchronize legal definitions for a more seamless fight against digital fraud. More importantly, adherence to internationally recognized frameworks fosters mutual trust and operational reciprocity among law enforcement agencies, thus reducing jurisdictional ambiguity in prosecuting cross-border cybercrimes. Such alignment strengthens the legal standing of electronic evidence for court proceedings and expedites the resolution of requests for mutual legal assistance. Additionally, Indonesia's active engagement in multilateral cyber regimes would enable the country to influence rule-making processes and ensure that its national interests are duly represented in shaping operational protocols. This international integration would also facilitate capacity-building initiatives through structured knowledge exchange and joint cyber exercises, consequently bridging domestic expertise gaps. The harmonization of domestic cybercrime legislation with global standards would enhance predictability and consistency in legal outcomes, fostering greater deterrence among potential perpetrators. Ultimately, delaying accession to pivotal cybercrime conventions perpetuates systemic vulnerabilities, inhibiting Indonesia's ability to respond decisively to rapidly evolving threats on the global digital stage.

Comparative analysis with systems in North America and Europe indicates that Indonesian reforms, though substantive, must be synchronized with investments in digital infrastructure, talent pipelines, and clear chains of command (Sudarwanto & Kharisma, 2023). Lessons from these jurisdictions point to the strategic importance of a central cybercrime authority, interoperable databases, and standing agreements for procedural cooperation. Moreover, the integration of advanced analytics and continuous digital skills training has proven vital in enhancing investigative capacity and adaptability within these advanced systems. Robust legal interoperability frameworks also facilitate the seamless transfer of evidence and accelerate multilateral investigations, thereby reducing procedural bottlenecks. The institutionalization of public-private partnerships has further enabled the rapid identification and neutralization of emergent threats, leveraging industry expertise to complement governmental oversight. Coordinated response mechanisms—backed by transparent protocols and systematic information-sharing—have been shown to minimize jurisdictional conflicts and improve case

resolution rates. Predictable funding allocations for cybercrime units are equally crucial, ensuring sustainable operational effectiveness and ongoing modernization of technological resources. The adoption of standardized incident reporting methods and continuous stakeholder engagement have strengthened collective situational awareness, contributing to a culture of vigilance and rapid threat mitigation. Ultimately, harmonizing Indonesia's reform agenda with proven global practices not only enhances national cyber resilience but also elevates its standing as a credible partner in international efforts to combat digital crime.

In summary, Indonesian legislative and institutional arrangements are marked by a commendable legal evolution but remain structurally and procedurally limited in addressing the full spectrum of transnational digital fraud. Gaps relating to cross-border evidence collection, institutional coordination, and integration with international norms indicate a need for multidimensional reform. Without accelerated legal harmonization and institutional modernization—including clear cross-agency mandates and capacity building—law enforcement will continue to be constrained by national borders in a global digital landscape.

Future legal reform must prioritize the creation of unified bodies for cross-border digital crime, the synchronization of statutes with leading international instruments, and the strengthening of technical and adaptive capacities. These measures will not only enhance prosecutorial efficacy and public confidence but will also fortify Indonesia's standing within the architecture of global digital governance.

CONCLUSION

National legal frameworks and institutional cooperation in addressing cross-border digital fraud remain constrained by the misalignment between prevailing statutory instruments and the practical demands of transnational arenas. The principal obstacles are rooted in weak inter-agency coordination, regulatory shortcomings in keeping pace with technological advancement and the rapid evolution of criminal modes of operation, and significant delays in harmonizing national norms with international standards and multilateral law enforcement mechanisms. These circumstances undermine the process of prosecuting offenders and restoring victims' losses, particularly when perpetrators act from outside national borders.

Legislative deficiencies and institutional fragmentation have generated vulnerabilities that can be exploited by fraud perpetrators while simultaneously prolonging the processes of extradition, asset tracing, and cross-border electronic evidence exchange. This situation underscores the need for fundamental reforms, including the adaptation to global conventions such as the Budapest Convention, the establishment of a centralized institution specializing in cybercrime, and the development of expedited mechanisms for mutual legal assistance. The existing fragility of the national legal apparatus in adapting to the shifting patterns of digital crime has the potential to erode public trust in online security and protection.

Future policy enhancement should prioritize the harmonization of national legal instruments with international frameworks, the establishment of an integrated national authority dedicated to combating digital crime, and significant capacity-building for human resources in digital forensics and law enforcement. These reforms must also be accompanied by investments in the development of cybercrime tracing technologies, improved accessibility for public reporting

and education, and the strengthening of procedures for cross-jurisdictional asset recovery and restitution. In turn, such measures would enable the domestic legal system to respond to cross-border digital crime in a more adaptive and coordinated manner.

REFERENCES

Ali, E. M., Dirgantara, F., & Darmawan, D. 2024. Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia. International Journal of Service Science, Management, Engineering, and Technology, 6(3), 27–38.

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. 2024. The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System. World Journal of Advanced Research and Reviews, 21(2), 205-217.

Anggriawan, R., & Susila, M. E. 2024. Legal Frontiers in the War Against Money Laundering: A Doctrinal Examination of Global Approaches. Jurnal Hukum Novelty, 15(2), 230-247.

Aryadi, D. W., Hardyansah, R., Darmawan, D., Saputra, R., Putra, A. R., Negara, D. S., & Maulani, A. 2024. Prosecution on Online Gambling Based on Enforcement of Criminal Law In Indonesia. International Journal of Service Science, Management, Engineering, and Technology, 5(2), 1–6.

Asghar, M. U., Javed, M. H., & Azhar, S. 2025. The Regulation of Cybercrime in International Law: Discussing the Legal Frameworks and Challenges in Regulating Cybercrime. Indus Journal of Social Sciences, 3(2), 417-430.

Ashurov, A. 2024. Jurisdictional Challenges in Cross-Border Cybercrime Investigations. Central Asian Journal of Multidisciplinary Research and Management Studies, 1(8), 22-30.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. 2023. Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. Journal of Social Science Studies, 3(1), 23–28.

Baraja, M. U., Saputra, R., Saktiawan, P., Dirgantara, F., & Waskito, S. 2023. Implementation and Supervision of Personal Data Protection Law on Online Platforms. Journal of Social Science Studies, 3(1), 101–108.

Buçaj, E., & Idrizaj, K. 2025. The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. Multidisciplinary Reviews, 8(1), 1-10.

Creswell, J. W., & Poth, C. N. 2018. Qualitative Inquiry and Research Design: Choosing among Five Approaches. Sage Publications, Thousand Oaks.

Fajria, N. C., & Ilmih, A. A. 2024. Kebijakan Perlindungan Data Pribadi dalam Menanggulangi Kejahatan Lintas Negara di Era Ekonomi Digital. Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora, 2(4), 16-24.

Flick, U. 2018. An Introduction to Qualitative Research. Sage Publications, London.

Kazandjiski, F. 2015. Investigation and Prosecution of Cyber Crime. TIJ's Research Journal of Social Science & Management - RJSSM.

Kumar, C. R. 2024. Cybercrime and the Law: Challenges in Prosecuting Digital Offenses. Indian Journal of Law, 2(5), 20-25.

Maksum, M. J. F. S. 2024. Legal Implications of Civil and Criminal Law on Investment Fraud Under the Guise of Online Business. Indonesian Economic Review, 4(1), 29-42.

Martono, M., Akbar, M. G. G., & Rahmatiar, Y. 2025. Law Enforcement of Transnational Cybercrime: Case Study in Indonesia. De Lega Lata: Jurnal Ilmu Hukum, 10(2), 279-286.

Panjaitan, M. D., Tarigan, A. I., Kembaren, I. Y. B., & Manalu, S. 2024. Impact of Extradition Agreement Policy on the State of Indonesia. Mimbar Keadilan: Jurnal Ilmu Hukum, 52-56.

Peters, A., & Jordan, A. 2019. Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. J. Nat'l Sec. L. & Pol'y, 10, 487.

Rahayu, N., Supriyono, I. A., Mulyawan, E., Nurfadhillah, F., Yulianto, D. R., & Ramadhan, A. Z. 2023. Pembangunan Ekonomi Indonesia dengan Tantangan Transformasi Digital. ADI Bisnis Digital Interdisiplin Jurnal, 4(1), 1-4.

Rusianto, R., Hardyansah, R., & Darmawan, D. 2023. Application of the Elements of Money Laundering Crime in Indonesian Jurisprudence. Bulletin of Science, Technology and Society, 2(3), 44–50.

Sahfitri, A., & Rosmalinda, R. 2024. Penipuan Digital Melalui Tautan Phishing. Jurnal Dialektika Hukum, 6(2), 92–107.

Sousa, E. S. 2023. Legal and Technical Challenges in the Pursuit of Cybercriminals: An Analysis of the Difficulties Faced by the Authorities. Seven Publicacoes Academicas, 1-7.

Stake, R. E. 2010. Qualitative Research: Studying How Things Work. Guilford Press, New York.

Sudarwanto, A. S., & Kharisma, D. B. 2023. Law Enforcement Against Investment Fraud: A Comparison Study from the USA and Canada with a Case Study on Binary Options in Indonesia. Safer Communities, 22(4), 235-253.

Wong, H. M. 2024. Research on International Cooperation in Cracking Down Cross-Border Cyber-Telecoms Fraud. Transactions on Social Science, Education and Humanities Research, 12, 8-14.

Yu, L., Cong, Q., & Li, S. 2024. Study on International Cooperation to Address Cross-Border Telecommunication Network Fraud Offence. J. Pol. & L., 17(2), 51-58.