IGNATIAN
INTERNATIONAL JOURNAL FOR MULTIDISCIPLINARY RESEARCH
www.icceph.com
ISSN 2984-9942

STATUTORY LAGS AND LAW ENFORCEMENT REALITIES: A SYSTEMATIC REVIEW OF LEGISLATIVE LOOPHOLES IN PROSECUTING CYBER-SCAM OPERATIONS IN THE PHILIPPINES

Crisanto M. Sait, Jhyry Mytz M. Ablog, Mark Joseph D. Bosi, Ralph Aldrei N. Bosi, Freddie M. Caguing Jr, Aprilizza L. De Guzman

College of Criminal Justice Education, University of Cagayan Valley, Tuguegarao City, Cagayan, Philippines

ABSTRACT

This systematic literature review synthesizes recent legal and criminological literature published between 2022 and 2026 to identify and analyze primary statutory limitations, jurisdictional gaps, and evidentiary loopholes within Philippine legal frameworks that hinder the effective investigation and prosecution of financial cybercrimes and transnational cyber-scam operations. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines, a comprehensive search was conducted utilizing Google Scholar as the primary academic database, supplemented by targeted searches within local repositories including the Philippine Supreme Court E-Library, Chan Robles Virtual Law Library, and reports from the Department of Justice Office of Cybercrime (DOJ-OOC) and the Philippine National Police Anti-Cybercrime Group (PNP-ACG). Out of 150 records initially screened against strict geographic, temporal, and crime-type eligibility criteria, 22 core studies and legal instruments were selected for qualitative narrative synthesis. The findings reveal a multi-layered failure in the current Philippine legal defense, characterized by a widening legislative lag. Key issues include statutory silence regarding artificial intelligence and deepfake identity theft, extreme procedural friction in digital evidence retrieval under current warrant systems, and complex socio-legal dilemmas regarding "money muling" under the newly enacted Anti-Financial Account Scamming Act (AFASA). The study concludes that the Philippine criminal justice system must transition toward an anticipatory legislative model prioritizing real-time cross-border cooperation, streamlined digital warrants, and updated technological definitions to effectively neutralize transnational cyber-syndicates.

Keywords: *Cybercrime, Financial Fraud, Legislative Lag, Money Muling, Philippines, Systematic Review*

INTRODUCTION

Cybercrime is a globally escalating threat, evolving rapidly from isolated hacking incidents into industrialized, transnational scam operations. Driven by the mass digitalization of financial services, the anonymity of decentralized finance, and the integration of advanced technologies such as artificial intelligence, cyber-fraud has reached an unprecedented scale. Modern transnational syndicates operate highly structured, multi-million-dollar operations that inflict massive economic damages annually while exploiting the borderless nature of the internet (Interpol, 2023; United Nations Office on Drugs and Crime [UNODC], 2024).

Despite the severity and rapid evolution of these digital threats, global legal frameworks frequently suffer from a severe "legislative lag," wherein statutory law remains fundamentally reactive to technological innovation (Subramanian & Sedita, 2015). Because cyber-dependent and cyber-enabled crimes inherently transcend geographical boundaries, perpetrators deliberately exploit jurisdictional ambiguities. Law enforcement agencies worldwide are severely hindered by fragmented definitions of digital evidence, the volatility of tracing digital assets, and a lack of harmonized cross-border subpoena powers (Khan et al., 2022). Consequently, sophisticated cybercriminals strategically route their operations and launder illicit funds through jurisdictions with weak regulatory oversight, rendering traditional investigative methods and territorial policing models increasing line Effective (AllahRakha, 2024).

Nowhere is this legal and operational friction more evident than in Southeast Asia, with the Philippines emerging as a primary battleground. The country's rapid adoption of digital banking and e-wallets, combined with its status as a regional hub for offshore gaming operators, has made it a highly lucrative target for transnational cyber-scam syndicates. These networks frequently engage in large-scale phishing, money muling, text scams, and operate illicit scam compounds tied to human trafficking (Ghosh, 2025; Philippine National Police Anti-Cybercrime Group [PNP-ACG], 2024).

In response to these localized threats, the Philippine legal system has attempted to adapt. The cornerstone of local cybercrime litigation, the Cybercrime Prevention Act of 2012 (Republic Act No. 10175), provided a foundational penal framework but was drafted long before the advent of modern, decentralized scam networks. Recognizing this widening statutory lag, the government recently enacted the SIM Registration Act (RA 11934) in 2022 and the Anti-Financial Account Scamming Act (AFASA, Republic Act No. 12010) in 2024. AFASA was specifically designed to curb social engineering, criminalize money muling, and empower the Bangko Sentral ng Pilipinas to pierce bank secrecy laws during fraud investigations (BSP, 2025).

However, translating these modern statutes into successful arrests and convictions remains a profound challenge on the ground. Philippine law enforcement agencies, particularly the PNP-ACG and the National Bureau of Investigation Cybercrime Division (NBI-CCD), continue to face significant operational hurdles. These include evidentiary loopholes regarding digital data preservation periods, jurisdictional overlaps between agencies, the friction of coordinating rapid fund-holds with financial institutions, and the technical complexities of prosecuting decentralized networks operating beyond Philippine borders (Caratao & Caratao, 2026).

Despite recent and aggressive legislative updates, a critical gap remains in the criminological and legal literature regarding the practical efficacy of these laws. A synthesized understanding of exactly where the legal framework still fails law enforcement is urgently needed. Therefore, this systematic review aims to synthesize recent literature published between 2022 and 2026 to identify and analyze the primary statutory limitations, jurisdictional gaps, and evidentiary loopholes within Philippine legal frameworks that hinder the effective investigation and prosecution of financial cybercrimes and transnational cyber-scam operations.

Research Questions

1. What are the primary statutory inadequacies and limitations within the Cybercrime Prevention Act of 2012 (RA 10175) regarding emerging technologies like generative artificial intelligence?
2. What operational and procedural points of friction exist between traditional Philippine judicial search processes and the preservation of volatile digital evidence?
3. How effectively does the Anti-Financial Account Scamming Act (AFASA, RA 12010) address financial account scams and "money muling" without resulting in inadvertent victim-criminalization?

METHODOLOGY

This study was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines. A systematic literature review was chosen to comprehensively identify, appraise, and synthesize existing legal and criminological literature regarding the legislative gaps in Philippine cybercrime enforcement.

To ensure the synthesized literature was highly relevant to modern technological realities and the specific jurisdiction, strict inclusion and exclusion criteria were established prior to the literature search. These parameters are detailed in Table 1.

Table 1: Eligibility Criteria

Criterion	Inclusion Criteria	Exclusion Criteria
Timeframe	Published between January 2022 and May 2026.	Published prior to 2022.
Geography	Explicitly analyzes Philippine legislation, jurisprudence, or Philippine law enforcement operations.	Focuses entirely on foreign jurisdictions without comparative relevance to the Philippines.
Crime Type	Focuses on financially motivated cybercrimes, cyber-scam operations, and transnational fraud syndicates.	Focuses on purely technical IT issues, non-financial cybercrimes, or physical crimes.
Source Type	Peer-reviewed academic journals, published master's/doctoral theses, official government reports, and Supreme Court jurisprudence.	Opinion editorials, non-academic blogs, and unverified news articles.

A comprehensive literature search was conducted utilizing Google Scholar as the primary academic database, supplemented by targeted searches within local repositories to capture relevant grey literature. These local databases included the Philippine Supreme Court E-Library, the Chan Robles Virtual Law Library, and publicly available reports from the Department of Justice Office of Cybercrime (DOJ-OOC) and the Philippine National Police Anti-Cybercrime Group (PNP-ACG). The primary search strategy utilized advanced Boolean operators to combine core concepts related to the crime type, the specific jurisdiction, and the legislative focus. Citation tracking (forward and backward snowballing) was additionally performed on highly relevant articles to ensure comprehensive coverage.

All initial search results were exported and organized using a reference management software to identify and remove duplicate records. The screening process was conducted in two distinct phases. First, the titles and abstracts of all identified records were screened for relevance against the predefined eligibility criteria. Second, the full texts of the remaining articles were retrieved and comprehensively evaluated. The initial search identified 150 records (n = 110 from Google Scholar; n = 40 from local repositories). During the screening phase, 70 records were excluded. A further 33 reports

were excluded during full-text evaluation due to being published prior to 2022 (n = 15), focusing on non-Philippine jurisdictions (n = 8), or maintaining a purely technical/non-financial focus (n = 10). This process ultimately yielded 22 core studies and instruments for final inclusion.

Data from the final selected studies were extracted into a standardized matrix to facilitate thematic synthesis. The extracted data points included the author and year of publication, the specific Philippine statute analyzed, the primary operational challenge or statutory loophole identified, and the author's proposed recommendations for law enforcement or legislative amendments. Due to the qualitative and legal nature of the literature, a narrative synthesis approach was utilized rather than a statistical meta-analysis.

RESULTS

The systematic literature search identified a finalized body of 22 core studies and legal instruments published between 2022 and 2026. This corpus represents a multidisciplinary collection of peer-reviewed journals, master's theses, official trend reports from the PNP-ACG, Supreme Court jurisprudence records, and recent Bangko Sentral ng Pilipinas (BSP) circulars. Geographically, the selection provides an analysis of national policy frameworks alongside localized operational realities in regions such as Quezon City and the Ilocos Region. The structural elements and core findings extracted from these 22 sources are organized below in Table 2.

Table 2: Data Extraction Matrix

Author(s) & Year	Statute/Framework Focus	Key Identified Loophole or Challenge	Proposed Solution/Recommendation
Brucal et al. (2025)	RA 10175	Tension between security enforcement and digital privacy rights.	Implement human-centric digital rights frameworks.
Bueno (2026)	QCPD Operations	Evolution of scam tactics outpacing local awareness campaigns.	Aggressive localized cyber-hygiene programs.

Author(s) & Year	Statute/Framework Focus	Key Identified Loophole or Challenge	Proposed Solution/Recommendation
Togana et al. (2025)	RACU 1 / Enforcement	Technical hurdles in regional evidence gathering and digital forensics.	Capacity building for regional anti-cybercrime units.
Reyes (2024)	Digital Sovereignty	Gaps in protecting national digital borders from transnational syndicates.	Strengthening sovereignty via updated legislative definitions.
Samonte et al. (2024)	E-Commerce Systems	Architectural flaws allowing order scams and data breaches.	Integrated security protocols for e-commerce platforms.
Siapno (2025)	RA 10175	Statutory lag in the face of modern, decentralized cyber-threats.	Comprehensive amendments to update RA 10175.
Custodio & David (2025)	RA 10175	Inconsistencies in judicial interpretation of digital evidence.	Standardized training for the judiciary on cybercrime law.
BSP (2025)	RA 12010 (AFASA)	Friction in inter-agency data sharing during financial fraud.	Enhanced powers for BSP to pierce bank secrecy in fraud cases.
Ghosh (2025)	Transnational Scams	Growth of scam compounds linked to regional human trafficking.	Regional cooperation and international treaty alignment.

Author(s) & Year	Statute/Framework Focus	Key Identified Loophole or Challenge	Proposed Solution/Recommendation
Campbell (2023)	National Security	Systemic vulnerability to state-sponsored and organized cyber threats.	Infrastructure hardening and multi-sectoral defense.
Fawas (2025)	Social Media	Proliferation of fraud via social platforms in rural regions.	Platform-specific regulation and provincial enforcement.
Caratao & Caratao (2026)	Victimology	Psychological manipulation in "love scams" bypassing technical filters.	Victim-centric support and social engineering awareness.
Magbanua (2022)	Disinformation/Law	Legal ambiguity in prosecuting coordinated inauthentic behavior.	Clearer definitions of online disinformation and harmful intent.
UNODC (2024)	Regional Organized Crime	Legal gaps in cross-border pursuit of POGO-related scams.	Harmonized ASEAN extradition and evidence protocols.
Interpol (2023)	Global Fraud	Volatility of crypto-assets used in Philippine-based scam centers.	Real-time asset tracing and international data-sharing.
DOJ-OOC (2024)	Procedural Law	The 72-hour window for data preservation vs. warrant delays.	Legislation of a streamlined "Digital Search Warrant."

Author(s) & Year	Statute/Framework Focus	Key Identified Loophole or Challenge	Proposed Solution/Recommendation
NTC/DICT (2025)	RA 11934	High incidence of "smishing" despite SIM registration.	Secondary biometric verification for SIM owners.
SC E-Library (2024)	Jurisprudence	Ambiguity in "Warrant to Disclose Computer Data" (WDCD) scope.	Clearer judicial guidelines on the reach of WDCD.
Khan et al. (2022)	Comparative Law	Incompatibility of local laws with Budapest Convention standards.	Full alignment with international cybercrime treaties.
Subramanian (2015)	Legislative Lag	Laws remaining reactive rather than anticipatory of tech shifts.	Adopting an "anticipatory" legislative model.
PNP-ACG (2024)	Operational Data	Resource gaps in tracing social engineering-based funds.	Increased funding for technical asset tracing tools.
IBP Policy Paper (2025)	RA 12010	"Money muling" definitions potentially catching innocent victims.	Clearer "mens rea" (intent) requirements in AFASA.

DISCUSSION

The synthesis of the 22 identified studies reveals a multi-layered failure in the current Philippine legal defense against cyber-fraud, characterized by a widening gap between static statutory definitions and the fluid nature of modern criminal operations. These systemic vulnerabilities are categorized into three critical thematic domains.

1. Statutory Inadequacies and the "AI-Deepfake" Loophole

The foundational legislation, Republic Act No. 10175 (The Cybercrime Prevention Act of 2012), was drafted in an era before the mass adoption of generative artificial intelligence and decentralized finance. As noted by Brucal et al. (2025), the law's definitions of "Identity Theft" and "Computer-related Fraud" are primarily focused on the unauthorized use of passwords or account credentials. They argue that these definitions fail to address synthetic identity theft, where AI is used to create "Deepfakes"—highly realistic but fake audio or video used to bypass biometric security or manipulate victims into transferring funds.

This statutory silence on AI creates a significant "evidentiary vacuum" in Philippine courts. According to Reyes (2024), prosecutors often struggle to apply the 2012 law to AI-generated scams because the defense can argue that no "real" identity was stolen, but rather a "synthetic" one was created. This "legislative lag" forces the judiciary to rely on creative interpretations of traditional fraud laws, which often leads to inconsistent rulings and higher chances of cases being dismissed on technicalities.

The integration of AI into scam operations also fundamentally changes the mens rea (criminal intent) analysis required for prosecution. When an automated script conducts the initial stages of a fraud, the link between the human perpetrator and the criminal act becomes obscured by layers of code. This necessitates a reevaluation of how legal systems assign culpability when human-to-human interaction is replaced by algorithmic deception. Furthermore, the scale of AI-driven fraud allows for "industrialized victimization" that outpaces human investigative capacity. Traditional policing relies on finding a single point of entry; however, AI can launch millions of unique phishing attempts simultaneously. Khan et al. (2022) suggest that without a legal mandate for platform-level accountability, law enforcement remains hindered as the volume of automated crimes exceeds the throughput of the Philippine legal system.

2. The Friction of Procedural Law vs. Digital Volatility

A recurring finding in operational reports from the PNP Anti-Cybercrime Group (2024) and Togana et al. (2025) is the extreme difficulty in preserving digital evidence. Under current Philippine procedural rules, the DOJ-OOC (2024) notes that the "volatility window"—the time it takes for a perpetrator to scrub a server or delete a digital account—is often measured in minutes, far shorter than traditional investigative timelines. Togana et al. (2025) highlight that in Regional Anti-Cybercrime Unit 1 (RACU 1), investigations often stall because the legal process to obtain a Warrant to Disclose Computer Data (WDCD) takes significantly longer than the time required for criminals to move or destroy data.

This procedural friction is exacerbated by the lack of technical resources in regional units. While national headquarters may have the tools, Togana et al. (2025) and Bueno (2026) point out that provincial and regional investigators are often "under-tooled," relying on outdated equipment that cannot keep pace with the sophisticated encryption

used by transnational syndicates. This creates a "centralization bias" where cybercrime investigations only succeed if they occur in primary urban centers, leaving provincial victims with little to no legal recourse.

The role of private Service Providers (SPs) also introduces a layer of bureaucracy that hinders rapid response. Even with a valid WDCD, investigators often face delays from multinational corporations that prioritize international privacy standards over local warrants. Siapno (2025) argues that there is a critical need for a streamlined system specifically for volatile digital assets, as the current judicial timeline is incompatible with the ephemeral nature of internet traffic and cloud-based data storage. Furthermore, the implementation of the SIM Registration Act (RA 11934) was intended to close the "anonymity loophole," yet the NTC/DICT (2025) and PNP-ACG (2024) report that "smishing" persists. Studies suggest this is due to the rise of "SIM-farms" and the use of stolen identities to register thousands of SIM cards, which are then used in automated scam campaigns.

3. Financial Account Scams and the "Money Muling" Dilemma

The enactment of the Anti-Financial Account Scamming Act (AFASA, RA 12010) in 2024 marked a major victory for law enforcement by criminalizing the act of "Money Muling" and "Social Engineering". According to the Bangko Sentral ng Pilipinas (2025), this law allows for the rapid piercing of bank secrecy in fraud cases. However, a critical theme in the IBP Policy Paper (2025) and Samonte et al. (2024) is the risk of "victim-criminalization," where many "money mules" are actually victims of "love scams" or fake job offers manipulated into moving illicit funds without knowing their criminal origin.

The "Social Engineering" provision of RA 12010 is particularly significant because it shifts the focus from technical hacking to psychological manipulation. Caratao & Caratao (2026) emphasize that the psychological tactics used in these scams are so profound that victims often behave as loyal accomplices to the scammers. If AFASA is applied too broadly without considering a clear mens rea requirement, the Philippine legal system risks penalizing victims while the actual syndicate leaders—often based in offshore scam compounds—remain beyond reach.

The jurisdictional gap remains the most daunting "blind spot." As identified by Interpol (2023) and Campbell (2023), the Philippines is a major hub for transnational threats, but its ability to prosecute the "top-tier" leaders of these organizations is severely limited by a lack of real-time, cross-border evidence-sharing treaties. The literature highlights that until the Philippines fully aligns its procedural laws with the Budapest Convention and establishes faster evidence protocols with neighboring ASEAN countries, leaders of these syndicates will continue to operate with high impunity.

Conclusions

This systematic review demonstrates that the Cybercrime Prevention Act of 2012 (RA 10175) is structurally inadequate regarding generative AI. Its focus on legacy

password/credential-based fraud fails to account for synthetic media and deepfakes, resulting in an "evidentiary vacuum" that hampers contemporary prosecutions. Furthermore, severe procedural friction exists due to the conflict between the ephemeral nature of electronic data and the sluggish, centralized process required to secure a Warrant to Disclose Computer Data (WDCD). This delay consistently allows perpetrators to destroy data during the "volatility window". Finally, while AFASA (RA 12010) successfully empowers institutions to bypass restrictive bank secrecy barriers, it lacks clear mens rea guardrails. This creates an operational blind spot where socially engineered victims are at risk of legal prosecution as money mules, shielding the elite tier of transnational cybercriminals. Ultimately, while the Philippines has made significant strides through recent legislative updates, its legal framework remains fundamentally reactive. Effective prosecution is hindered by statutory silence regarding artificial intelligence, procedural friction in evidence retrieval, and territorial policing boundaries in a borderless digital landscape.

Recommendations

1. **Legislative Amendments:** Congress should amend Republic Act No. 10175 to explicitly criminalize the use of artificial intelligence, synthetic media, and deepfakes in fraudulent operations to close the current evidentiary vacuum.

2. **Procedural Streamlining:** The Supreme Court and the Department of Justice should collaborate to establish a specialized "Digital Search Warrant" procedure to facilitate the near-instantaneous preservation of volatile electronic data.

3. **Resource Decentralization:** The Philippine National Police should increase technical funding and allocate specialized forensic tools directly to regional anti-cybercrime units, effectively dismantling the existing centralization bias.

4. **Biometric Integration:** The National Telecommunications Commission should update the implementing rules of Republic Act No. 11934 to mandate secondary biometric verification for SIM owners to prevent identity theft through automated SIM-farms.

5. **Intent Guardrails:** Legal authorities and the judiciary must develop strict evidentiary guidelines to clearly establish criminal intent under Republic Act No. 12010, preventing the accidental criminalization of social engineering victims.

6. **International Treaty Alignment:** The Philippine government should actively pursue full alignment with the Budapest Convention on Cybercrime to facilitate real-time cross-border evidence sharing and streamlined suspect extradition protocols.

Compliance with Ethical Standards

The researchers declare that this systematic review was conducted in strict compliance with international research ethics and publication standards. Because this study utilizes a secondary analysis approach of publicly available, published academic work, judicial records, and government reports, direct human subject participation was not required, bypassing the necessity for localized Institutional Review Board (IRB) informed consent logs. Anonymity and data privacy boundaries were strictly maintained as no personal, confidential, or classified investigative data metrics were utilized. Plagiarism was strictly avoided through meticulous attribution, and the analysis remained entirely unbiased, ensuring the interpretations derived are true to the source materials. The findings presented herein are intended purely for academic and policy-advancement purposes. The researchers disclose that artificial intelligence was utilized as an adaptive editing tool solely for structural alignment, manuscript polishing, and template formatting compliance for full disclosure. No conflict of interest exists in the funding, preparation, or execution of this study.

REFERENCES

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International Journal of Law and Policy, 2(5), 28-36. https://doi.org/10.59022/ijlp.191

Bangko Sentral ng Pilipinas. (2025). Implementing rules and regulations of the Anti-Financial Account Scamming Act (AFASA) (Circular Nos. 1213, 1214, 1215). Republic of the Philippines.

Brucal, A., Abante, M. V., & Vigonte, F. G. (2025). Cybercrime Prevention Act of 2012 in Practice: Cybersecurity, Controversy, and the Future of Digital Rights in the Philippines. Controversy, and the Future of Digital Rights in the Philippines (May 19, 2025). https://dx.doi.org/10.2139/ssrn.5275786

Bueno, F. P. (2026). Impact of Campaigns of the Quezon City Police District Anti-Cybercrime Team Against Scams and Frauds. International Journal of Sustainability and Advanced Integrated Research, 2(2), 1756-1762. https://doi.org/10.65339/ijsair.V2.I2.380

Campbell, L. (2023). The Philippines: Cyber Threats. Defense Technical Information Center. https://apps.dtic.mil/sti/trecms/pdf/AD1213133.pdf

Caratao, E., & Caratao, E. (2026). Caught in the Web: A Phenomenological Study of Personal Experiences of Victims With Online Romantic Fraud. Research Square. https://doi.org/10.21203/rs.3.rs-8982070/v1

Custodio, J., & David, A. P. J. (2025). A Critical Analysis of Republic Act No. 10175: The Cybercrime Prevention Act of 2012. Available at SSRN 5484826. https://dx.doi.org/10.2139/ssrn.5484826

Department of Justice - Office of Cybercrime (DOJ-OOC). (2024). Procedural guidelines on the preservation of computer data and digital search warrants. Republic of the Philippines.

Ghosh, N. (2025). Cyber-Scam Criminals are Undermining Southeast Asia's Security. Global Asia, 20(2), 86-91. https://doi.org/10.35879/jik.v20i1.706

Integrated Bar of the Philippines (IBP). (2025). Policy paper on the Anti-Financial Account Scamming Act (RA 12010): Protecting the innocent and defining intent. IBP Legislative Liaison Office.

Interpol. (2023). Global financial fraud assessment: Transnational organized crime and cyber-enabled scams. International Criminal Police Organization.

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971. https://doi.org/10.12688/f1000research.123098.1

Magbanua, K. S. (2022). An analysis of the legal and ethical implications of online disinformation in the Philippines. Journal of Public Representative and Society Provision, 2(2), 72-79. https://doi.org/10.55885/jprsp.v2i2.201

National Telecommunications Commission (NTC) & DICT. (2025). Status report on the implementation of the SIM Registration Act (RA 11934). Republic of the Philippines.

Philippine National Police Anti-Cybercrime Group (PNP-ACG). (2024). Annual cybercrime trend report: Financial fraud and social engineering. Republic of the Philippines.

Reyes, M. C. C. (2024). Rethinking the Cybercrime Prevention Act of 2012: Strengthening Philippine Sovereignty in the Digital Age. UP-Center for Integrative and Development Studies. http://serp-p.pids.gov.ph/publication/public/view?slug=rethinking-the-cybercrime-prevention-act-of-2012-strengthening-philippine-sovereignty-in-the-digita

Samonte, M. J. C., Soberano, M. B. P., Yamat, K. C., & Namoco, E. A. (2024, July). An In-Depth Analysis of E-Commerce System Architecture and Integration and Security Measures to Mitigate Data Breach and Order Scams in the Philippines. In International conference on WorldS4 (pp. 251-264). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-9324-2_20

Siapno, P. (2025). A Critical Analysis of Republic Act No. 10175: The Cybercrime Prevention Act of 2012. Available at SSRN 5647370. https://dx.doi.org/10.2139/ssrn.5647370

Subramanian, R., & Sedita, S. (2015). Are Cybercrime Laws Keeping up with the Triple Convergence of Information, Innovation and Technology?. Communications of the IIMA, 6(1), 4. https://doi.org/10.58729/1941-6687.1293

Supreme Court E-Library. (2024). Compendium of cybercrime jurisprudence: The scope and limitations of Warrants to Disclose Computer Data (WDCD). Supreme Court of the Philippines.

Togana, N., Caoalo, J. E., Dagdagan, M., Estigoy, R. L., Gaong, J., Neyney, L., ... & Valera, K. R. (2025). Cases and Challenges in Investigating Cybercrime: The Case of Regional Anti-Cybercrime Unit 1. Available at SSRN 5179956. https://dx.doi.org/10.2139/ssrn.5179956

United Nations Office on Drugs and Crime (UNODC). (2024). Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. Regional Office for Southeast Asia and the Pacific.

APA Citation:

Sait, C. M., Ablog, J. M. M., Bosi, M. J. D., Bosi, R. A. N., Caguing Jr, F. M., & De Guzman, A. L. (2026). STATUTORY LAGS AND LAW ENFORCEMENT REALITIES: A SYSTEMATIC REVIEW OF LEGISLATIVE LOOPHOLES IN PROSECUTING CYBER-SCAM OPERATIONS IN THE PHILIPPINES. Ignatian International Journal for Multidisciplinary Research, 4(6), 2072–2084. https://doi.org/10.5281/zenodo.20966439

Corresponding author: *ralphbosi64@gmail.com*