January - June 2025 Volume 34 Issue 1 PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW

Official Publication of Medicolegal Association of Maharashtra

MULTISPECIALITY, MULTIDISCIPLINARY, NATIONAL
PEER REVIEWED, OPEN ACCESS, MLAM (SOCIETY) JOURNAL
Indexed with Scopus (Elsevier)

Editorial Office Address
Department of Forensic Medicine & Toxicology, Third Floor, Library Building, Seth G S Medical College & KEM Hospital, Parel, Mumbai, Maharashtra, India. Pin-400 012. Email id: mlameditor@gmail.com Phone: 022-24107620 Mobile No. +91-9423016325.

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW
(Official Publication of Medicolegal Association of Maharashtra)
Email.id: mlameditor@gmail.com

PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

Short Communication

Insoluble Challenges of Prosecuting Transnational Cybercrime: A Case in a Developing Country

Oanh Thi Cao[a*], Tuan Van Vu[b]
[a]Assoc. Prof. Oanh Thi Cao, Faculty of Criminal Law, Hanoi Law University, Hanoi, Viet Nam. Email: caothioanh@gmail.com. https://orcid.org/0009-0007-1423-2426. [b]Assoc. Prof. Tuan Van Vu, Faculty of Legal Foreign Languages - Hanoi Law University, tuanvv@hlu.edu; https://orcid.org/0000-0002-3066-7338

Article Info

Received on: 04.05.2025
Accepted on: 05.06.2025

Key words
Cybersecurity Resources,
Insoluble Challenges
Legal Gaps,
Transnational Cybercrime.

Abstract

Introduction: Transnational cybercrime includes hacking, phishing, identity theft, ransomware, and cyber espionage conducted across national borders. Its borderless nature complicates jurisdiction, investigation, and prosecution, particularly in developing countries such as Vietnam, where legal and institutional gaps remain acute. **Methods:** This qualitative, descriptive study employed secondary sources to analyze the multifaceted challenges of prosecuting and preventing cybercrime in developing contexts, with Vietnam as a case study. **Results:** Findings reveal that limited resources, outdated laws, weak forensic capacity, and corruption hinder effective enforcement. Jurisdictional ambiguity and technological deficits further constrain prosecutions. The medicolegal dimension heightens risks: breaches of healthcare systems and electronic health records compromise privacy, patient safety, and evidentiary integrity, engaging both civil liability and professional accountability. **Conclusion:** Addressing these challenges requires harmonized legislation aligned with international standards, specialized cybercrime units, medicolegal safeguards, and robust international cooperation. Public awareness and societal resilience remain critical to securing the digital environment.

1. Introduction

The Transnational cybercrime refers to criminal activity conducted through digital networks that transcend national borders, complicating investigation and prosecution due to divergent laws, priorities, and resources.[1] Such offences are often perpetrated by organized networks exploiting jurisdictional fragmentation to evade liability. Developing countries encounter heightened vulnerability, given resource constraints, infrastructural deficits, and legal lacunae.[2] As Clough[3] notes that the borderless nature of the Internet enables cybercriminals to target regions with weak cybersecurity regimes, confident that enforcement capacity is limited.

How to cite this article: Oanh TC, Tuan VV. Insoluble Challenges of Prosecuting Transnational Cybercrime: A Case in a Developing Country. J Forensic Med Sci Law. 2025;34(1):60-63. doi: 10.59988/jfmsl.vol.34issue1.12

***Corresponding author:** Oanh Thi Cao, Faculty of Criminal Law – Hanoi Law University, 87 Nguyen Chi Thanh street, Giang Vo district, Hanoi city, Vietnam. Email: oanhhs@hlu.edu.vn

Cybersecurity infrastructure in these jurisdictions is further undermined by shortages of skilled professionals, inconsistent regulations, and competing political priorities. Corruption within enforcement agencies exacerbates this deficit, while low public awareness and poor cyber hygiene among citizens make individuals and enterprises particularly susceptible to phishing, ransomware, and identity theft.[4] Natarajan and Androulaki[5] emphasize that political instability or competing national interests often result in cybersecurity being deprioritized, creating fertile ground for exploitation.

The medicolegal dimension raises distinctive concerns. Breaches of healthcare databases, telemedicine platforms, and hospital systems jeopardize not only informational privacy but also patient safety. Unlawful access may facilitate insurance fraud, manipulation of medical histories, or disruption of clinical care, thereby implicating both civil liability and professional accountability.[6] Developing countries must, therefore, embed medicolegal safeguards into their frameworks, including statutory duties of confidentiality, malpractice-style liability standards for cybersecurity lapses in medical institutions, and formal recognition of electronic health data as a protected evidentiary category.[7] Vietnam illustrates both progress and persistent gaps. Legislative developments such as the 2018 Cybersecurity Law[8] and Decree No. 53/2022/ND-CP,[9] alongside partnerships with INTERPOL, ASEAN, and UNODC, reflect a commitment to transnational collaboration. Nevertheless, limited resources, a cybersecurity skills gap, and inadequate public awareness continue to impede effective prevention.[10] A multi-faceted approach, such as legal reform, professional training, infrastructural investment, medicolegal integration, and sustained international cooperation, remains indispensable. This paper aimed to answer the following questions:

1. What laws and regulations has Vietnam implemented to combat transnational cybercrime?
2. What challenges does Vietnam face in implementing and enforcing transnational cybersecurity regulations?

2. Methods

This study employed a structural review research design based on a qualitative analytical approach proposed by Linos and Carlson[11] for law writing review methods. It also examined secondary sources and emphasized systematic data collection, transparency, and ethical considerations to contribute to rich, contextually grounded insights into the challenges of imposing legal sanctions on transborder criminality in developing countries like Vietnam.

3. Discussion

3.1. Challenges in prosecuting transnational cybercrime in Vietnam

Transnational cybercrime prosecution is inherently complex because of the borderless nature of the Internet, divergent legal regimes, and the increasing sophistication of offenders' methods. In developing countries like Vietnam, the challenges of such an approach are exacerbated by jurisdictional ambiguity, technological deficits, and limited institutional capacity.[10] The lack of explicit statutory provisions on extraterritorial jurisdiction frequently impedes prosecutorial authority, especially in cases that offend multiple sovereigns. Effective prosecution thus necessitates legal reform alongside active participation in bilateral and multilateral instruments, extradition, and cross-border exchange of evidence.[12] Resource constraints further weaken enforcement capabilities because offenders use anonymization, encryption and darknets beyond the current forensic and investigative capabilities. Insufficient budgets limit investment in digital forensic laboratories, advanced surveillance technologies, and judicial training in cyberlaw.[13] Without such assistance, law enforcement agencies lack the tools to even identify, retain, and present intricate electronic evidence. Parallel efforts in public awareness campaigns are also crucial to encourage early reporting and prevention.[7]

From a medicolegal standpoint, issues of evidentiary integrity and procedural compliance are critical. Digital evidence must satisfy chain-of-custody requirements and admissibility standards consistent with both domestic law and international privacy regimes, such as GDPR-inspired frameworks.[14] Accordingly, courts must consider the extent to which collected evidence extraterritorially complies with Vietnamese rules of procedure and evidence, as any failure to meet this will likely lead to exclusion and consequent collapse of prosecutions. Forensic practitioners, moreover, bear ethical and legal duties to ensure impartiality, accuracy, and confidentiality, thereby protecting the rights of the accused while upholding prosecutorial legitimacy.[15] There are also political and institutional obstacles, such as corruption, bureaucratic inefficiency, and insufficient

judicial independence that make it difficult to apply regulations effectively. Strengthening governance, transparency and accountability of investigative and prosecuting authorities is still essential.[4] Ultimately, the effective prosecution of transnational cybercrime in Vietnam requires a holistic strategy combining legislative harmonization, forensic preparedness, international cooperation, and medicolegal safeguards, thereby enhancing prosecutorial efficacy and digital security resilience.

3.2. Implications for combating and preventing transnational cybercrime in Vietnam

It is necessary to have a harmonised and practical instrument to combat and prevent transnational cybercrime in developing countries, including Vietnam. In today's digital age, cybercrime routinely transcends territorial boundaries, rendering traditional jurisdictional doctrines inadequate absent meaningful reform.[7] From the perspective of substantive criminal law, Vietnam's existing provisions regulate certain cyber-offences but fail to capture the expanding spectrum of digital threats, including ransomware schemes and intrusions into critical infrastructure. As Roscini explains, the lack of clearly defined terms, proportionate penalties, and uniform procedural protections undermines deterrence and compromises justice.[2] Consequently, harmonisation with foreign legal frameworks, particularly the Budapest Convention on Cybercrime, would increase both the jurisdictional reach, admissibility of digital evidence and compliance with internationally recognised due process principles. The medicolegal aspect emphasizes further vulnerabilities.[15] Cyberattacks against healthcare systems, telemedicine platforms, and repositories of electronic health records are related to privacy, patient safety, and public health. Violations may enable identity theft, insurance fraud, and manipulation of medical histories, so these breaches implicate civil liability and professional responsibility.[16,17] In contrast, a combined medicolegal approach is needed to be instituted as a matter of law in Vietnam. This would involve statutory duties of confidentiality for healthcare institutions, liability standards analogous to medical malpractice for cybersecurity lapses, and recognition of digital health records as a protected evidentiary category in judicial proceedings.

In terms of institutional capacity, enforcement remains constrained by deficits in forensic expertise and limited technological resources. Establishing specialized cybercrime units, which are supported by sustained investment in forensic technologies and professional training, is indispensable.[18] The incorporation of forensic medicine and health-law experts into investigative processes would further strengthen the State's capacity to address crimes targeting medical infrastructure and patient data. Because of the transnational character of cybercrime, unilateral domestic action is insufficient. It is necessary for Vietnam to participate in multilateral processes, including INTERPOL, UNODC, and ASEAN cyber initiatives, for the purposes of intelligence exchange, mutual legal assistance, and extradition.[5] As a result, harmonized standards on evidence preservation and medicolegal certification will strengthen cross-border enforcement.[13] Finally, it is important to emphasize the role of societal resilience. As reported by the Ministry of Public Security, public unawareness of cyber risks increases susceptibility to fraud, identity theft, and medical data misuse.[10] Besides, nationwide educational initiatives, which are integrated into curricula and reinforced by campaigns, are therefore critical. Public confidence in reporting mechanisms also promotes incident detection and strengthens prosecutorial outcomes.[15] Overall, a comprehensive strategy combining legal reform, medicolegal accountability, institutional strengthening, and international cooperation is essential for developing states confronting transnational cybercrime.

4. Conclusion

Transnational cybercrime poses profound challenges for developing countries such as Vietnam, where legal gaps, resource limitations, and jurisdictional fragmentation undermine effective enforcement. While Vietnam has advanced through its Cybersecurity Law, Decree No. 53/2022/ND-CP, and collaboration with INTERPOL, ASEAN, and UNODC, significant obstacles remain, including limited forensic capacity, a shortage of skilled professionals, and low public awareness. The medicolegal dimension illustrates the heightened risks to healthcare systems, telemedicine, and electronic health records, where breaches compromise privacy, patient safety, and evidentiary integrity. To address these risks, statutory duties of confidentiality, malpractice-style liability standards, and recognition of digital health data as protected evidence must be integrated into the legal framework. Sustainable progress requires a comprehensive approach: harmonized legislation,

specialized enforcement units, forensic preparedness, public education, and cross-border cooperation. Only by embedding medicolegal safeguards within a broader cybersecurity strategy can Vietnam enhance resilience and ensure justice in the face of evolving cyber threats.

Ethical Clearance: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organization.

Contributor ship of Author: All authors equally contributed.

Conflict of interest: None to declare.

Source of funding: None to declare.

Acknowledgments: The author would like to thanks Hanoi Law University for their supports of this research.

References:

1. Rajasekharaiah KM, Dule CS, Sudarshan E. Cyber security challenges and its emerging trends on latest technologies. IOP Conf Ser Mater Sci Eng. 2020;981(2):022062.
2. Bada A, Nurse JR. Transnational cybersecurity: A review of the legal framework and challenges. Comput Secur. 2020;95:101812.
3. Clough J. Principles of cybercrime. Cambridge: Cambridge University Press; 2015.
4. Nance K, Smith M. The emerging transnational nature of cyber threats: Challenges and strategies. J Int Aff. 2018;72(1):51-70.
5. Natarajan M, Androulaki E. Challenges to policing transnational cybercrime: Lessons from INTERPOL's initiatives. Policing Soc. 2018;28(4):451-65.
6. Raed SAF. Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. Int J Cyber Criminol. 2023;17(2):77-94.
7. Wall DS. Transnational cybercrime: Issues of jurisdiction and enforcement. Eur J Crim Policy Res. 2022;28(4):597-616.
8. National Assembly of Vietnam. Cybersecurity law, Law No.24/2018/QH14 [Internet]. Hanoi: National Assembly; 2018 [cited on 28th Oct 2024]. Available from: https://vanban.chinhphu.vn/?pageid=27160&docid=206114
9. Government of Vietnam. Decree elaborating a number of the law on cybersecurity of Vietnam, No.53/2022/ND-CP [Internet]. Hanoi: Government of Vietnam; 2022 [cited on 28th Oct 2024]. Available from: https://vanban.chinhphu.vn/?pageid=27160&docid=206381
10. Do QH, Tuan VV, Tuan AL. Current challenges in need of more stringent sanctions to combat increasing high-tech crimes in a developing country in the age of fourth industrialization. Int Law Soc Res. 2024; 8(1):433-62.
11. Linos K, Carlson M. Qualitative methods for law review writing. Univ Chic Law Rev. 2017;84(1):213-38.
12. Do HV, Bui TH. High-tech crime in the banking and finance field in the context of Industry 4.0: Current situation and solutions. VITAI. 2024;7(4).
13. Broadhurst R, Chang LYC. Cybercrime in Asia: Trends and challenges. London: Routledge; 2021.
14. Choucri N. Cyberpolitics in international relations. Cambridge: MIT Press; 2018.
15. Van DJ, Jansen M. Cybersecurity in a global context: The role of international cooperation. Comput Secur. 2021;104:102164.
16. Singh SN, Singh D, Dev K, Mittal AK, Srivastava A. Anti-forensics: Tool against cyber forensic. J Forensic Med Sci Law. 2023; 32(1):68-73.
17. Deokar RB, Patil SS. Artificial Intelligence in Healthcare and Biomedical Research - Ethical aspects. J Forensic Med Sci Law. 2024; 33(1):1-4.
18. Chang LYC, Grabosky P. The governance of cybercrime in Asia: Harmonization of law and policy. Crime Law Soc Change. 2017;67(2):201-14.