

Comparative Study of Cybercrime Laws in Emerging Economies

Dr Anand Kumar Dwivedi

Assistant Professor

Department of Law

VSSD college Kanpur 208002

Orcid id: <https://orcid.org/0009-0009-8256-1074>

Abstract— The proliferation of digital technologies across emerging economies has created unprecedented opportunities for economic growth, financial inclusion, and social connectivity, while simultaneously exposing these nations to escalating cybercrime risks. This manuscript undertakes a comparative analysis of cybercrime legislation across select emerging economies, namely India, Nigeria, and other developing jurisdictions tracked by international bodies such as the United Nations Conference on Trade and Development (UNCTAD). The study examines the structure, scope, and enforcement mechanisms of these laws, identifies common gaps such as weak institutional capacity, jurisdictional ambiguity, and inconsistent international cooperation, and evaluates the extent to which national frameworks align with global standards. Drawing on verifiable legal instruments, government publications, and peer-reviewed literature, the paper concludes that while legislative adoption in emerging economies has improved substantially over the past two decades, enforcement, capacity-building, and cross-border harmonization remain the most pressing unresolved challenges.

Keywords— cybercrime, emerging economies, cyber law, digital governance, comparative legal analysis, enforcement, cybersecurity policy

INTRODUCTION

The expansion of internet penetration, mobile banking, and e-commerce in emerging economies has been accompanied by a parallel rise in cyber-enabled offences, including financial fraud, identity theft, data breaches, and cyberterrorism. Unlike developed economies, many emerging markets adopted cybercrime legislation later, often as a reactive measure following high-profile incidents rather than as part of a proactive regulatory strategy. This has resulted in fragmented legal frameworks that vary considerably in their definitions of offences, procedural safeguards, and enforcement infrastructure.

Emerging economies face a distinctive set of challenges: rapid digitization outpacing regulatory capacity, limited technical expertise within law enforcement agencies, resource constraints

for cross-border investigation, and tension between national security imperatives and the protection of civil liberties. At the same time, several emerging economies—India, Nigeria, Indonesia, and others—have made significant legislative strides, establishing dedicated cybercrime statutes, computer emergency response teams, and specialized prosecutorial units. A comparative study of these frameworks is valuable not only for identifying best practices but also for understanding the structural barriers that continue to hinder effective cyber governance in the Global South.

This manuscript compares the legal architecture of cybercrime regulation in selected emerging economies, situates these frameworks within the broader global cyberlaw landscape as tracked by UNCTAD, and proposes recommendations for legislative and institutional reform.



LITERATURE REVIEW

Scholarship on cybercrime law in emerging economies has grown substantially, reflecting the urgency of the subject. A comparative legal analysis of cyber law situates the regulatory approaches of leading digital economies against evolving technological threats, noting that legal systems in leading digital economies such as the United States, the European Union, and China have adapted differently to challenges posed by AI, blockchain, and IoT, reflecting divergent regulatory philosophies and enforcement mechanisms. This body of work also emphasizes the role of international collaboration in

combating transnational cybercrime and addressing regulatory fragmentation in a globalized digital economy, a theme highly relevant to emerging economies that often lack the institutional weight to negotiate multilateral cyber-governance arrangements.

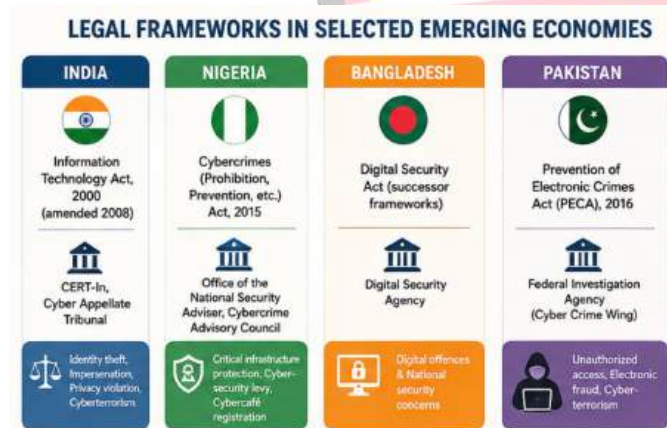
Research focused specifically on South Asia offers a useful comparative lens. A study of cybercrime legislation in India, Bangladesh, and Pakistan finds that although these countries share the common objective of safeguarding digital integrity and security, their laws differ considerably in scope, enforcement mechanisms, and adherence to public law principles such as transparency, accountability, and the protection of fundamental rights. The same research further notes significant gaps in regional harmonization that hinder effective cross-border cooperation against transnational cybercrime, reinforcing the argument that legislative adoption alone does not guarantee regional cyber-resilience.

Comparative work covering multiple jurisdictions has also examined landmark statutes and case law shaping the field. One such comparative review discusses foundational statutes including India's Information Technology Act 2000, the U.S. Computer Fraud and Abuse Act of 1986, the EU's General Data Protection Regulation, and China's Cybersecurity Law of 2017, alongside landmark judicial decisions such as *Shreya Singhal v. Union of India* and *Google v. CNIL* that have shaped cyber legal developments. It concludes by advocating greater international harmonization of cyber norms, collaborative enforcement mechanisms, and proactive legislative reforms tailored to technological advancement.

for policy design in other emerging regions. Similarly, comparative research on Gulf Cooperation Council countries finds that despite sharing common legal traditions, GCC states differ meaningfully in the substantive content of their anti-cybercrime statutes.

Global data compiled by UNCTAD provides the most systematic empirical foundation for comparative cyberlaw research. According to UNCTAD's most recent cyberlaw survey, by the end of 2021, 71 percent of countries globally had adopted data-protection legislation, up from 55 percent in 2015, while the share of countries with cybercrime and consumer-protection laws rose by nine percentage points over the same period. However, the survey also shows persistent disparities: while 79 percent of developing countries, including 70 percent of least developed countries, had adopted cybercrime laws, fewer than half of least developed countries had corresponding privacy legislation. An earlier UNCTAD release similarly reported that 79 percent of countries worldwide had cybercrime legislation, with adoption highest in Europe at 89 percent and lowest in Africa at 72 percent, while cautioning that developing countries often lack sufficient resources for enforcement even after laws are formally adopted.

At the national level, Nigeria's principal cybercrime statute illustrates a common legislative model adopted across emerging economies. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 was enacted to provide an effective, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. Analysis of the Act's implementation notes that its passage followed years of reliance on ordinary evidentiary and criminal statutes, since the absence of a dedicated cybercrime legal framework had hampered effective criminal justice measures until the 2015 Act came into force. Critical appraisals of the statute observe that although it is comprehensive—containing 59 sections across eight parts, including schedules establishing a Cybercrime Advisory Council and a Cyber-security Fund—the Act nonetheless contains loopholes that require urgent legislative amendment. A subsequent review of the law's implementation record notes that a provision of the Act was challenged before the ECOWAS Court, which ordered the Nigerian government in a 2020 judgment to repeal or amend Section 24, a ruling the government did not implement until 2024, illustrating the gap between legislative text and enforcement compliance.



Regional studies on Africa reinforce the finding that legislative existence and enforcement effectiveness are distinct issues. A systematic review of cybercrime enforcement in Africa concludes that enforcement effectiveness is primarily shaped by institutional and technological constraints rather than the absence of legal frameworks, a finding with direct implications

India's Information Technology Act, 2000, together with its 2008 amendment, represents one of the earliest comprehensive cyber statutes among emerging economies. Legal commentary notes that the 2008 amendment introduced Sections 66A through 66F, covering offences including identity theft, cheating by impersonation, violation of privacy, and cyber

terrorism, while also granting the government authority under Section 69 to intercept, monitor, or decrypt information transmitted through computer systems. However, the amendment's expansion of speech-related offences proved controversial: analysis of the statute's judicial history shows that Section 66A, which criminalized sending offensive electronic messages, was struck down by the Supreme Court of India in the 2015 Shreya Singhal case for violating the constitutional guarantee of free speech. Commentary on the amendment further observes that it has drawn criticism because it decreased penalties for some cybercrimes and was seen as lacking sufficient safeguards for civil rights, with one cyber-law expert quoted as characterizing the surveillance powers under Section 69 as giving the Indian government a character resembling that of a surveillance state.

Collectively, this literature demonstrates three recurring findings relevant to emerging economies: first, legislative adoption rates have risen markedly over the past two decades but remain uneven across regions; second, the mere existence of a cybercrime statute does not guarantee effective enforcement, given resource and institutional constraints; and third, cybercrime laws in emerging economies frequently generate tension between security objectives and the protection of fundamental rights, a tension resolved differently across jurisdictions through judicial review, legislative amendment, or continued executive discretion.

RESEARCH OBJECTIVES

- To examine the structural and substantive features of cybercrime legislation in selected emerging economies.
- To identify common strengths, weaknesses, and enforcement gaps across these frameworks.
- To assess the extent of alignment between national cybercrime laws and international standards.
- To propose policy recommendations for strengthening legislative and institutional capacity in emerging economies.

RESEARCH METHODOLOGY

This study adopts a doctrinal and comparative legal research methodology. Primary sources include the text of national cybercrime statutes—such as India's Information Technology Act, 2000 (as amended in 2008) and Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act, 2015—alongside official reports published by international organizations, particularly UNCTAD's Global Cyberlaw Tracker. Secondary sources comprise peer-reviewed and practitioner legal literature examining the implementation and judicial interpretation of

these statutes. The comparative method is used to identify convergences and divergences in statutory scope, enforcement architecture, and rights-protection mechanisms across jurisdictions.

Legal Frameworks in Selected Emerging Economies

Country	Principal Legislation	Year Enacted	Key Institutions	Notable Provisions
India	Information Technology Act, 2000 (amended 2008)	2000 / 2008	CERT-In, Cyber Appellate Tribunal	Sections 66A–66F on identity theft, impersonation, privacy violation, cyberterrorism; Section 69 interception powers
Nigeria	Cybercrimes (Prohibition, Prevention, etc.) Act	2015	Office of the National Security Adviser, Cybercrime Advisory Council	Critical infrastructure protection, cyber-security levy, cybercafé registration
Bangladesh	Digital Security Act (successor frameworks to earlier ICT laws)	2018	Digital Security Agency	Provisions addressing digital offences and national security concerns
Pakistan	Prevention of Electronic Crimes Act (PECA)	2016	Federal Investigation Agency (Cyber Crime Wing)	Offences relating to unauthorized access, electronic fraud, cyberterrorism

Comparative Analysis

Dimension	India	Nigeria	Regional/Global Pattern (UNCTAD)
Legislative maturity	Foundational law dates to 2000; amended 2008	Enacted later, in 2015	Developing countries show 79% adoption of cybercrime laws
Judicial oversight	Active; Section 66A struck down by Supreme Court (2015)	Provision challenged before ECOWAS Court (2020 ruling)	Judicial review of rights-restrictive provisions remains uneven globally
Enforcement capacity	CERT-In and specialized cyber units, but resource strain persists	National Security Adviser coordination; enforcement gaps noted in scholarship	Africa records lowest regional adoption (72%) and weakest enforcement capacity
Rights security balance	Criticized for surveillance powers under Section 69	Section 24 challenged as rights-restrictive	Persistent global tension between security provisions and civil liberties

International cooperation	Limited formal harmonization with regional neighbors	AU Convention referenced as an alignment benchmark	Cross-border enforcement identified as a leading unresolved challenge
---------------------------	--	--	---



DISCUSSION

The comparative evidence indicates that emerging economies have made substantial legislative progress in criminalizing cyber-enabled offences, yet significant disparities persist in the quality of enforcement and the protection of constitutional rights. India's experience demonstrates the value of an active judiciary in checking executive overreach, as seen in the invalidation of Section 66A. Nigeria's experience illustrates how regional judicial bodies, such as the ECOWAS Court, can serve as an external check on domestic legislation, although compliance with such rulings may be delayed for years. Both cases underscore that legislative texts alone are insufficient; independent oversight mechanisms are essential to ensuring that cybercrime laws do not become instruments of disproportionate state control.

The UNCTAD data further situates these national experiences within a broader global pattern: while cybercrime legislation has diffused rapidly across developing and least-developed countries, complementary areas such as data protection and consumer protection lag considerably, and enforcement capacity—particularly for cross-border investigation—remains the most acute deficiency identified across regional studies of Africa, South Asia, and the Gulf.

CHALLENGES AND GAPS

- Weak technical and institutional capacity for digital forensics and cybercrime investigation.
- Jurisdictional ambiguity in prosecuting transnational offences.

- Tension between national-security-oriented surveillance provisions and constitutional rights to privacy and free expression.
- Delayed or inconsistent compliance with judicial and regional rulings mandating legislative amendment.
- Uneven regional harmonization, limiting the effectiveness of cross-border cooperation mechanisms.

RECOMMENDATIONS

- Strengthen judicial and parliamentary oversight mechanisms to review cybercrime provisions for proportionality and rights compliance.
- Invest in specialized training and digital forensic infrastructure for law enforcement agencies.
- Pursue regional harmonization initiatives, drawing on frameworks such as the African Union Convention on Cybersecurity and Personal Data Protection.
- Establish clear, technology-neutral statutory definitions to reduce the need for frequent legislative amendment.
- Enhance international cooperation mechanisms, including mutual legal assistance treaties tailored to cyber-enabled offences.

CONCLUSION

Cybercrime legislation in emerging economies has evolved considerably over the past two decades, moving from an absence of dedicated statutes toward comprehensive, if imperfect, legal frameworks. The comparative analysis of India and Nigeria, situated within the broader empirical landscape documented by UNCTAD, reveals that legislative adoption has outpaced enforcement capacity and rights-protection safeguards in many jurisdictions. Addressing this gap will require not only continued legislative reform but sustained investment in institutional capacity, judicial oversight, and regional and international cooperation mechanisms tailored to the realities of emerging economies.

REFERENCES

1. Cyber Law in a Globalized World: A Comparative Analysis Through the Lens of Law and Society. ResearchGate, 2024. <https://www.researchgate.net/publication/385588404>
2. Comparative Study of Cyber Laws in Different Countries. International Journal of Law, Law and Legal Research (IJLLR), 2025. <https://www.ijllr.com/post/comparative-study-of-cyber-laws-in-different-countries>
3. Comparative Public Law and Cyber Law Governance: A Study of Cybercrime Legislation in India, Bangladesh and Pakistan. Academia.edu, 2025. <https://www.academia.edu/128138809>

4. Assessing the Effectiveness of Cybercrime Laws in Africa: A Systematic Review of Enforcement Barriers and Policy Reform Options. Udechukwu, C.C. ResearchGate. https://www.researchgate.net/figure/Percentage-of-countries-with-cybercrime-legislation_fig1_362880995
5. A Comparative Study of Anti-Cybercrime Laws in the Gulf Cooperation Council Countries. IEEE Xplore. <https://ieeexplore.ieee.org/document/7905281/>
6. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. UNODC/ICT Policy Africa. <https://ictpolicyafrica.org/fr/document/h52z5b28pir>
7. Nigeria Country Profile. Octopus Cybercrime Community, Council of Europe. https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/nigeria/pop_up
8. Understanding Nigeria's Cybercrimes Act and its Implementation Mechanism. Ogun, F. Centre for Journalism Innovation and Development. <https://thecjid.org/understanding-nigerias-cybercrimes-act-and-its-implementation-mechanism/>
9. A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria. ISRCL, 2021. <https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf>
10. Global Cyberlaw Tracker. UN Trade and Development (UNCTAD). <https://unctad.org/page/cybercrime-legislation-worldwide>
11. Least Developed Countries Still Lag Behind in Cyberlaw Reforms. UNCTAD, 2022. <https://unctad.org/news/least-developed-countries-still-lag-behind-cyberlaw-reforms>
12. Data and Privacy Unprotected in One Third of Countries, Despite Progress. UNCTAD, 2020. <https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress>
13. Information Technology Amendment Act 2008 (IT Act 2008). TechTarget. <https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008>
14. Strengthening India's Cybersecurity Framework: IT Laws and Rules. Journalism University, 2026. <https://journalism.university/digital-media/india-cybersecurity-framework-it-laws-rules/>
15. Navigating the Information Technology Act 2000: India's Legal Shield Against Cyber Vulnerabilities. TheLaw.Institute, 2026. <https://thelaw.institute/privacy-and-data-protection/information-technology-act-2000-india-cyber-law/>

