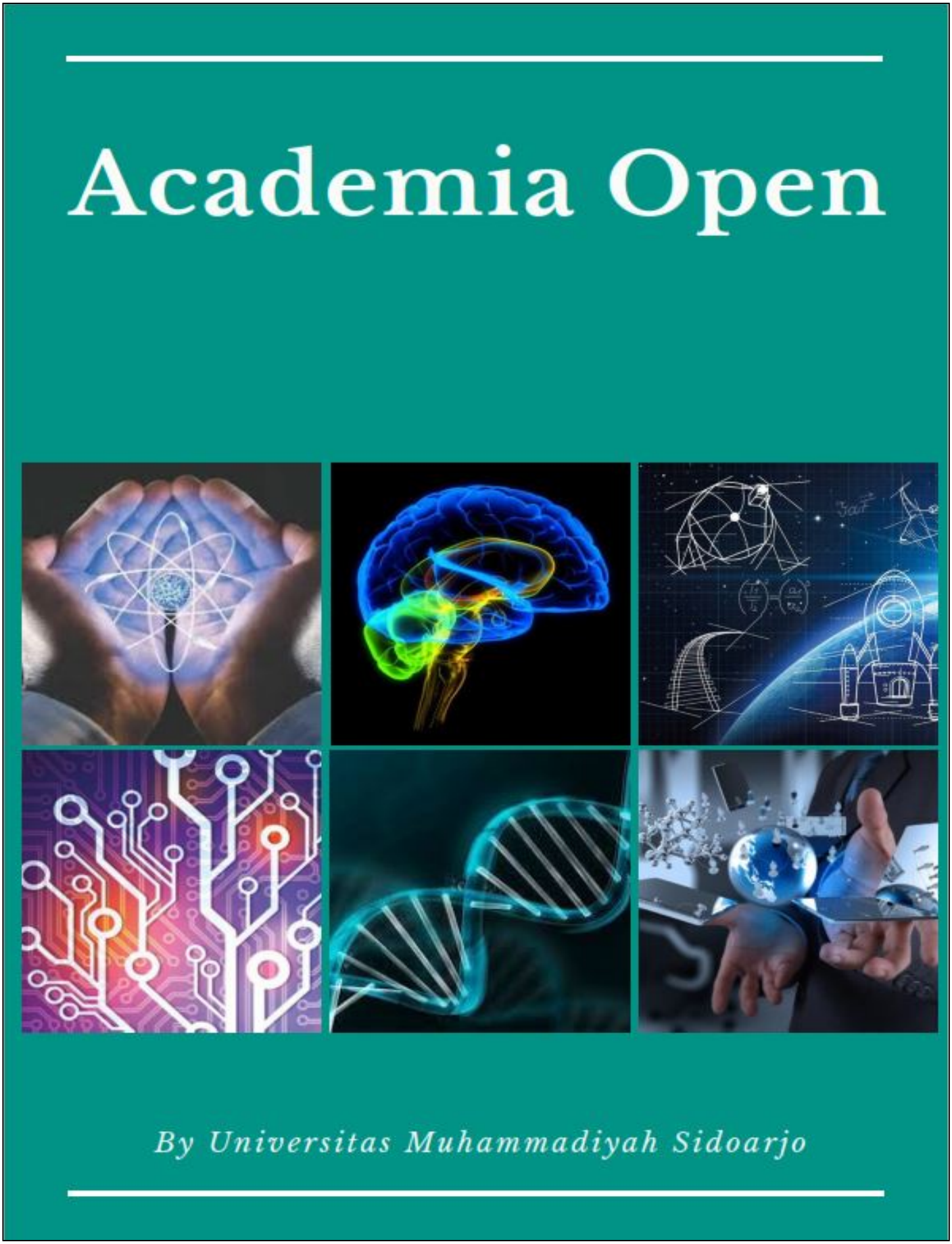
Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)

Table Of Content

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)



ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)

EDITORIAL TEAM

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)

Evolving Legal Responsibilities and Challenges in Prosecuting Cybercrime Across Jurisdictions

Tanggung Jawab Hukum yang Berkembang dan Tantangan dalam Menindak Kejahatan Dunia Maya di Seluruh Yurisdiksi

Riyadh Hussain Taqi, mriyadh44@yahoo.com, (1)
College of Nursing, University of Basrah, Basrah, Iraq

(1) Corresponding author

Abstract

General Background: In the digital age, cybercrime has emerged as a sophisticated and transnational threat, endangering global security, economic stability, and individual privacy. **Specific Background:** The rapid evolution of cyber-offenses challenges traditional legal frameworks, particularly in defining liability and proving criminal intent in virtual environments. **Knowledge Gap:** Despite ongoing reforms, there is limited clarity on how legal systems conceptualize and apply core criminal law principles such as *actus reus* and *mens rea* to cybercrime, particularly across diverse jurisdictions. **Aims:** This study investigates the evolving definitions of criminal responsibility in cybercrime, analyzes the adaptation of legal systems to digital threats, and explores the evidentiary challenges in proving guilt within cyberspace. **Results:** The findings confirm that while *actus reus* and *mens rea* remain applicable, their interpretation in digital contexts becomes significantly complex. Key challenges include jurisdictional disputes, offender anonymity, and digital evidence admissibility. **Novelty:** Through doctrinal and comparative legal research, this study presents a multi-jurisdictional analysis spanning the U.S., E.U., Asia, and the Middle East, offering a comprehensive perspective on legal convergence in addressing cybercrime. **Implications:** Legal systems must innovate by enacting precise cybercrime statutes, investing in digital forensic capabilities, enhancing professional education, and fostering global legal harmonization to ensure effective cyber justice.

Highlights:

1. Redefining Crime Elements: Adapting *actus reus* and *mens rea* digitally.
2. Legal Reform Needed: Update laws, boost digital investigation capacity.
3. Global Coordination Required: Harmonize international laws for cybercrime enforcement.

Keywords: Cybercrime, Criminal Responsibility, Digital Evidence, Comparative Law, Legal Reform

Published date: 2025-04-29 00:00:00

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.10842 . Article type: (Law)

Introduction

Digital expansion has brought a complete transformation to communication methods and both education systems and government functions, and business activities. Digital expansion has made many illegal business transactions [1]. Cybercrime represents the illegal execution of digital offenses through computing devices and network systems, which include hacking, along with identity theft, online fraud, cyberstalking, data breaches, and other digital transgressions [2].

The specific feature that distinguishes cybercrime from classic criminal activity is its simultaneous invisibility, instantaneous, and worldwide functionality [3]. The ability for hackers based in a single country allows them to intercept data belonging to people and businesses throughout multiple continents. Legal systems today face numerous questions about cybercrime because identities behind encrypted networks remain hidden. Do we have a way to establish the intentions of unidentified attackers who hide under encryption? In modern digital systems, which parties need to be held accountable remains an unresolved question [4].

Methods

This research is based on:

-Doctrinal Legal Research: A close reading of criminal codes, cybercrime legislation, and international treaties.

-Comparative Legal Analysis: A comparison between how different jurisdictions— such as the United States, the European Union, and selected countries in Asia and the Middle East—address criminal liability in cybercrime cases.

-The researcher performed a qualitative data review on scholarly literature and official reports, and published case law from 2010 through 2024.

-The study did not gather any experimental interview data or statistical information. The study analyzes law through interpretation exclusively without any additional elements.

Result and Discussion

Results

Legal Elements of Criminal Responsibility in Cybercrime

-The requirement for establishing criminal liability includes accomplishing these two fundamental requirements:

-The elements of guilty actions in cybercrime generally include unauthorized access and illegal data retrieval, and deploying ransomware and distributed malicious software programs.

-Identifying guilty criminal mindsets through Mens Rea remains challenging when examining cybercrime situations. Remote control operations combined with automated malicious scripts create dubious intentions regarding criminal activity.

The following table summarizes common categories of cybercrime, including descriptions and real-world examples:

Type of Cybercrime	Description	Examples
System Hacking	Unauthorized access to devices or networks	Breaching government or banking systems
Identity Theft	Illegally using someone else's personal information	Using another person's ID number or bank card
Online Financial Fraud	Illegitimately obtaining money through the internet	Phishing emails, fake bank transfers
Malware Distribution	Spreading viruses or spyware to harm or steal data	Ransomware, keylogger programs
Cyber Extortion	Threatening to release data unless a ransom is paid	Threatening to publish private photos unless paid
Digital Defamation / Threats	Using the internet to harm reputation or issue threats	Online slander campaigns on social media

Table 1.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Challenges in Attribution and Prosecution

1. Cybercriminals employ anonymously positioned proxies together with Virtual Private Networks (VPNs) to use dark web networks for maintaining their hidden identities.

2. Cybercrime victims from multiple countries cause jurisdictional problems because authorities must determine which nation should prosecute the offenders.

3. The process of handling digital evidence for court starts with specialized collection and moves to preservation, then ends with court presentation, requiring expert tools which many jurisdictions lack.

4. The laws regarding cybercrime often present turbulent problems because outdated legislation permits either frivolous prosecutions of innocent activities or fails to prosecute genuine cybercrimes.

The following table provides estimated global distribution data about significant cybercrime categories for a better understanding of the types that need immediate legal action.

Type of Cybercrime	Estimated Percentage of Total Cybercrimes
Financial Fraud	35%
Hacking	25%
Extortion/Defamation	15%
Identity Theft	10%
Malware Attacks	10%
Others	5%

Table 2.

Judicial and Legislative Responses

-Several jurisdictions now have laws that address particular cyber offenses, including the Computer Fraud and Abuse Act in the United States.

-Through the Budapest Convention, nations can access international cooperation tools which aid cybercrime investigations as well as prosecutions between countries.

-Investigative authorities use ethical hacking and malware analysis together with blockchain tracking as advanced digital investigation tools.

-Archived digital data which includes IP logs together with email headers and metadata and expert witness statements now obtains legitimation as valid court evidence.

Law / Convention	Issuing Body	Main Objective
Budapest Convention	Council of Europe	Harmonize laws and assist countries in combating cybercrime
U.S. DOJ Cybercrime Guidelines (2022)	United States Department of Justice	Prosecute federal cybercrime cases
China’s Cybersecurity Law	Government of China	Regulate internet use and protect national security
Saudi Anti-Cybercrime Law	Kingdom of Saudi Arabia	Define and criminalize cyber offenses, and protect information

Table 3.

Discussion

Legal concepts related to criminal responsibility within cybercrime require modern evaluation for effective application [5]. The required components of criminal law remain applicable, but become more obscure to trace alongside the progression of online criminal activities [6].

The prosecution faces challenges in proving intent because defendants claim unawareness of illegal conduct, especially when determining illegality in complex coding or tool usage situations. A teenager might acquire hacking software without knowing that doing so amounts to a criminal offense [7].

Attribution is another challenge. Under what circumstances does a legal responsibility cascade when various

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

parties collaborate on a cyberattack? Does someone need an identified human being to commit such an act if autonomous bots can carry it out? The current state of laws is unable to resolve legal ambiguities that stem from various complex cyberattacks. Nationwide cyberattacks face obstacles due to conflicting privacy regulations and sovereign rights, and data protection concerns among different countries. The legal ability to touch a cybercriminal exists only within one nation because there are no extradition agreements between states [8].

As digital evidence usage grows in courts, it creates problems regarding maintaining chain of custody standards as well as authenticity and technical reliability of computer evidence [9]. People who serve as judges and jurors often lack sufficient technical knowledge to validate digital evidence, thus creating opportunities for inaccurate decision-making or wrongful imprisonment [10].

Conclusion

Criminal responsibility concepts in cybercrime remain in development. Criminal responsibility in cybercrime pushes legal systems to transform both their statutory laws and their investigation procedures and judicial processes. Lawful frameworks need to fulfill following requirements to guarantee both equity and operational excellence.

New laws must provide both precise definitions for cybercrimes along their punishment guidelines.

•Invest in digital forensic capabilities.

Legal authorities need proper education about cyber laws for professional development.

International collaboration strategies combined with unified legal guidelines should be implemented by governments across the world.

-The complex digital environment demands that justice systems evolve at the same speed to preserve the possibility of holding offenders accountable for their computer-based crimes.

References

1. O. E. COUNCIL, "Convention on Cybercrime, Budapest, 2001," ed.
2. I. Citaristi, "United Nations Office on Drugs and Crime—UNODC," in The Europa Directory of International Organizations 2022, ed: Routledge, 2022, pp. 248-252.
3. M. Bianucci, T. Mahesh, J. Mallory, J. Tsoi, and J. Warren, "Computer Crimes," Am. Crim. L. Rev., vol. 59, p. 511, 2022.
4. A. M. Aminu, "International criminal police organisation and the challenges in the fight against cybercrime in Nigeria," Kashere Journal of Politics and International Relations, vol. 2, pp. 48-56, 2024.
5. H. Chander and G. Kaur, Cyber laws and IT protection: PHI Learning Pvt. Ltd., 2022.
6. A. ASSESSMENT, "European Union," 2013.
7. R. G. Smith, R. Sarre, L. Y.-C. Chang, and L. Y.-C. Lau, Cybercrime in the pandemic digital age and beyond: Springer, 2023.
8. M. N. I. Khan, "CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES," American Journal of Scholarly Research and Innovation, vol. 4, pp. 138-174, 2025.
9. V. Singh and A. K. Singh, "An Analysis of Cyber Laws with Focus on Data Protection in India: Issues, Challenges, and Opportunities," Jus Corpus LJ, vol. 3, p. 254, 2022.
10. V. A. Kumar, S. Bhardwaj, and M. Lather, "Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms," Productivity, vol. 65, pp. 1-10, 2024.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo