SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 9484-9490
Open Access. Online & Print

DOI: 10.5281/zenodo.20379704

CYBERCRIME AND DIGITAL POLICING: LEGAL CHALLENGES IN THE ERA OF TECHNOLOGICAL ADVANCEMENT

Dr. Pushkar Shankar Shukla[1*], Dr Kranti Deshmukh[2], Yashika Manchanda[3], Dr. Kuldeep Kaur[4], Dr. Pramod Vishwakarma[5], Dr Sidhartha Sekhar Dash[6]

[1]LLB, LLM, PhD, MATS University, Raipur Email - pushkarss@rediffmail.com*
[2]Associate Professor, Marathwada Mitra Mandals Shankarrao Chavan Law College, Savitribai Phule Pune University, Email ID - kranti.deshmukh@rediffmail.com, Orcid I'd: 0009-0006-5287-4983
[3]PhD Scholar, Faculty of Law, SRM University Delhi NCR, Sonipat, Haryana, Email ID: yashikamanchanda05@gmail.com
[4]Assistant Professor, Cinema Studies and Journalism and Media, Department of Journalism and Media Studies, Multani Mal Modi College, Patiala- 147001, Punjab, India, Email Id: Kuldeep.modicollege@gmail.com, Orcid Id: 0009-0008-8413-0553
[5]Associate Professor, AIT-CSE, Chandigarh University, Mohali-140413, Punjab, India. Email ID - pramod.e9758@cumail.in Orcid I'd: 0000-0002-8020-9554
[6]Associate Professor, School of Law, Kiit Deemed to be University, Email ID: sidharthadash.1981@gmail.com

Received: **16/12/2025**
Accepted: **02/02/2026**

Corresponding Author: Pushkar Shankar Shukla (pushkarss@rediffmail.com)

Abstract
The rapid advancement of digital technologies has significantly transformed both the nature of cybercrime and the mechanisms of law enforcement, giving rise to complex legal and regulatory challenges. This study examines the evolving intersection between cybercrime and digital policing, with a particular focus on the adequacy of existing legal frameworks in addressing technologically driven threats. Adopting a qualitative doctrinal and comparative research design, the study analyzes key legal issues, including jurisdictional limitations, attribution difficulties, and challenges related to the admissibility of digital evidence. It further evaluates the implications of emerging digital policing tools such as artificial intelligence, predictive analytics, and surveillance technologies on fundamental rights, including privacy and due process. The findings reveal a persistent gap between rapid technological innovation and the capacity of legal systems to regulate it effectively, resulting in regulatory fragmentation and increased risks to civil liberties. Through a comparative analysis of India, the European Union, and the United States, the study highlights divergent regulatory approaches and the absence of harmonized global standards. The research proposes the development of an adaptive techno-legal framework that balances security imperatives with accountability and human rights protections. The study contributes to cyber law scholarship by offering critical insights for policymakers and advancing the discourse on digital governance in the contemporary era.

Keywords: *Cybercrime, Digital Policing, Cyber Law, Artificial Intelligence, Surveillance, Jurisdiction, Data Protection, Digital Evidence*

1. Introduction

The quick rise of digital ecosystems has caused a significant transformation in nature, scale, and intricacy of criminal activities globally. Cybercrime has not remained one hacking attempt or fraud trick but rather has taken form of transnational

criminality that is associated with ransomware attacks, cyber-terrorism, identity thefts, and increasingly involves cyber-attacks based on the use of artificial intelligence (Meghana et al., 2024; Atrey, 2023). As a result, cybercriminals have become able to carry out more complex criminal acts faster and more anonymously, hence causing a lot of difficulties for the traditional law enforcement through application of advanced technologies such as machine learning, automation, and big data analysis (Meghana et al., 2024; Atrey, 2023). In view of the ever-increasing interactivity of digital systems in different spheres of economic, political, and social activity, the opportunities for committing cyber-crimes have expanded substantially, creating a new problem for both national security and international governance (AllahRakha, 2024).

Digital devices and technologies have become popular tools in the hands of law enforcers responding to the new threat. Digital policing, with its use of AI-based surveillance systems, predictive policing, and other digital technologies, represents a radical change in police activities (Montasari, 2023). There are numerous advantages to utilizing these technologies in terms of efficiency and real-time crime detection and prevention. However, their implementation poses several legal and ethical questions (Place, 2018). The algorithms used as the basis of the decision-making process as well as vast data collection pose the problems of transparency, accountability, and potential systematic discrimination, thereby complicating the issue of legitimacy in democratic policing processes (Akpobome, 2024).

Despite the technological advancement, the current legislation remains highly underdeveloped to address the problem of cybercrime and implications associated with digital policing. Traditional legislation and its principles including territorial jurisdiction and physical evidence prove inefficient in addressing issues related to the intangible and nonterritorial nature of cyberspace (Savaş and Karataş, 2022). Cybercrime attribution, cross-border law enforcement, and the question of the admissibility of digital evidence pose major challenges to contemporary legal systems (Saxena and Mayank, 2020). The increasing use of advanced technologies also aggravates the conflict between ensuring the security of the state and protecting the fundamental rights of citizens, including privacy and due process. The increase in surveillance opportunities, which are often not accompanied by effective mechanisms to control them, poses critical concerns of proportionality, need, and the danger of power abuse (Bhatti, 2024; Bassini, 2019).

Even though the past studies have made great strides in the research on cybercrime and digital policing, much of the literature addresses these two concepts individually. The situation with technological innovation and legal regulation is an underresearched topic in the literature, as scholars are more likely to concentrate on specific elements of the phenomenon such as cybersecurity regulations, digital evidence, or surveillance (Pandey, 2023; Savaş and Karataş, 2022). This divided approach inhibits the emergence of approaches to the problem that could be able to handle the complexity of the interaction of cybercrime and digital policing. Additionally, comparative legal analyses across regions are relatively underdeveloped, yet this knowledge would play a vital role in understanding how different regulatory mechanisms respond to the same problems within the context of increasing globalization.

It is within this context that there would be an urgent need for an integrated techno-legal analysis, which would be able to bridge the gap between technological advancement and legislation. This is vital if an adequate legal framework sensitive to the changing needs of today is developed in order to respond to the new challenges without affecting the rights of citizens. It will be another contribution to the vast body of research on the matter of cyber law and digital governance. More specifically, it will address issues concerning cybercrimes and digital policing by critically analyzing legal issues associated with this phenomenon.

Research Objectives

1. To analyze key legal challenges in regulating cybercrime in technologically advanced environments
2. To assess the impact of digital policing on legal frameworks and fundamental rights
3. To propose an adaptive techno-legal framework for effective and rights-compliant regulation

2. Methodology

2.1 Research Design

The study uses the qualitative doctrinal research design in order to analyze the legal issues concerning cybercrime and digital policing. The use of the qualitative doctrinal design makes it possible for the legal principles, the existing statutory laws, and the interpretation of the same to be explored systematically. Given that the issue is multidisciplinary, other forms of research that can be used include policy research and techno-legal research. The qualitative doctrinal design is particularly ideal in uncovering any weaknesses in

the existing legal frameworks as well as their efficiency in handling technology-driven problems.

2.2 Data Sources

This study will be based both on primary and secondary sources so that the coverage on the research problem could be comprehensive. As far as the primary sources are concerned, the statutory instruments such as the Information Technology Act, 2000, GDPR, and Budapest Convention, and the case law will be viewed as important ones. In turn, the secondary sources will include the literature on the subject (the works that have been published in peer-reviewed journals, as well as the reports released by other international organizations such as UNODC, Europol, and Interpol).

2.3 Analytical Framework

The thematic analysis method is useful to investigate the main legal issues related to cybercrime and digital policing. It is analyzed based on the thematic categories, the challenge of jurisdiction, the challenge of attribution, the challenge of the admissibility of digital evidence, and the conflict between surveillance and fundamental rights. The given methodology enables assessing how the legal systems react to the technological development in a logical way. Moreover, it facilitates the identification of the patterns and peculiarities of the legal regulation of cybercrime and digital policing.

2.4 Comparative Legal Analysis

In the case of this particular study, comparative analysis between three different legal jurisdictions has been conducted. These three legal jurisdictions are India, the European Union, and the United States. Such selection has been done due to the fact that each of the above jurisdictions uses varied methods to regulate cyber laws internationally. Comparative analysis helps identify any gaps in regulation as well as best practices. Moreover, it serves to get a wider picture about how other legal jurisdictions handle the issue of cyber law.

2.5 Limitations of the Study

The study acknowledges some of the limitations associated with the research design and methodology. Given the nature of change and development, the rapid dynamics in technology and cybersecurity could be light-years ahead of what the law currently has to offer, which would affect the relevancy of the findings in the long run. In addition, the opaque nature of technological tools used in digital policing, especially those based on algorithms, makes it impossible to get an insight into the operational processes, making it difficult to conduct a quantitative evaluation. However, despite these limitations, the study provides quality qualitative findings.

3. Results

3.1 Jurisdictional and Regulatory Gaps in Cybercrime Law

Based on the findings, one of the biggest hurdles to the regulation of cybercrimes lies in jurisdiction. The traditional territorial-based legal system framework, shown in Table 1 below, does not seem to be capable of handling crimes committed in more than one jurisdiction. In addition, the differences in legal systems across various countries and the uneven adoption of international tools make the enforcement process harder. Although there exist conventions such as the Budapest Convention that provide an opportunity for cooperation, their limited geographical coverage renders them ineffective. The loopholes created are then manipulated by cybercriminals for their own gain.

Table 1: Jurisdictional and Regulatory Challenges in Cybercrime

Issue	Description	Implication
Territorial Jurisdiction	Laws confined to national boundaries	Ineffective cross-border enforcement
Legal Fragmentation	Variations in cyber laws across countries	Lack of harmonization
Limited International Adoption	Partial adoption of global conventions	Weak cooperation mechanisms
Regulatory Arbitrage	Exploitation of legal loopholes across jurisdictions	Increased cybercrime risks

3.2 Challenges in Attribution and Digital Evidence

The paper proposes that the main hindrances of the prosecution of cybercrime cases are the process of attribution and evidentiary challenges. Encryption and anonymity are some of the technologies that prevent the identification of the culprit as shown in Table 2. Moreover, the adoption of inconsistent standards, when authenticating the digital evidence in different jurisdictions, minimises the credibility of the court process. Issues of data integrity and chain of custody also add to the complexity of the issue of evidence admissibility. The results imply that current evidentiary models fail to deal with technical challenges of cybercrime investigations.

Table 2: Attribution and Digital Evidence Challenges

Issue	Description	Implication
Anonymization Tools	Use of VPNs, Tor networks	Difficulty in identifying offenders
Encryption Technologies	Secured communication channels	Limited access to evidence
Chain of Custody Issues	Handling and preservation of digital data	Questionable evidence reliability
Legal Inconsistencies	Variations in evidentiary standards	Weak prosecution outcomes

3.3 Legal and Ethical Concerns in Digital Policing

Implementation of digital police technology brings a lot of legal and ethical concerns, namely the issues of accountability and transparency. As shown in Table 3, algorithms employed in such systems are unexplainable; therefore, they are more likely to produce bias results. Also, it is a problem that is exacerbated by the lack of guidelines on the use of artificial intelligence in policing. Moreover, as surveillance tools are on the rise, there is a lack of sufficient means to safeguard individuals against power abuse. These results imply that there is an urgent necessity of regulation and governance structures.

Table 3: Legal and Ethical Issues in Digital Policing

Issue	Description	Implication
Algorithmic Bias	Bias in AI decision-making systems	Discriminatory outcomes
Lack of Transparency	Opaque functioning of predictive algorithms	Reduced accountability
Regulatory Gaps	Absence of clear laws governing AI in policing	Legal ambiguity
Surveillance Expansion	Increased use of monitoring technologies	Risk of misuse of authority

3.4 Impact on Fundamental Rights

Findings point to the existence of a significant gap between the implementation of digital policing and the protection of the key human rights. Such increased surveillance and data gathering have far-reaching impact on privacy and data security as shown in Table 4 below. Moreover, there is the possibility that introduction of such technological innovations may hamper due process especially by decreasing human intervention in decision-making processes. Inadequate legal safeguards make this threat even more dangerous, since there is a possibility that constitutional principles could be violated.

Table 4: Impact on Fundamental Rights

Issue	Description	Implication
Privacy Violations	Mass data collection and surveillance	Erosion of individual privacy
Data Protection Risks	Weak safeguards in handling personal data	Increased vulnerability
Due Process Concerns	Automated decision-making in policing	Reduced fairness
Lack of Oversight	Absence of accountability mechanisms	Potential abuse of power

3.5 Comparative Insights Across Jurisdictions

It is clear from the comparison that the regulatory methods vary greatly between the jurisdictions. The EU concentrates on ensuring strong protection of the data and rights-based regulation while US is characterized by a fragmented regulatory method, which is shown in Table 5 below. On the contrary, India has not yet developed its legal framework and it encounters problems in enforcement. These discrepancies point out the absence of a global approach to dealing with cybercrime and digital policing. The findings show that there needs to be a global standard.

Table 5: Comparative Legal Approaches

Jurisdiction	Key Features	Strengths	Limitations
European Union	GDPR-based, rights-focused	Strong data protection	Operational constraints
United States	Sector-specific regulations	Flexibility	Lack of uniformity
India	Emerging legal framework	Growing regulatory focus	Enforcement and capacity gaps

4. Discussion

The findings from this paper indicate the existence of an intrinsic structural problem in the legal systems' approach to addressing cybercrime and digital policing amid rapid technological advancements. Fragmented jurisdictions and inconsistent regulation identified in the findings continue to act as a barrier to effective law enforcement, thus confirming the notion that conventional ideas about territorial sovereignty

have become increasingly less relevant in the context of cyberspace (Afzal,2024). This discord has become a well-known feature of contemporary legal discourse, where the definition of cyber sovereignty has been shifting and what impact it has on international law (Chatinakrob, 2024; Tsagourias, 2021). The continued existence of territorially-based legal systems as exemplified in Table 1 also points to the dire necessity of the redefinition of jurisdiction outside the physical plane.

Attribution and digital evidence is another case, where traditional principles of law are rather limited. Lack of the ability to unambiguously blame perpetrators of computer crimes and the inability to employ digital evidence weakens criminal justice systems. These results could be regarded as a manifestation of the problem of inefficiency of the evidence standards prevailing in the technological environment. Along with making investigations of crime more challenging, the rising use of encryption and anonymization technologies makes the normative issues of privacy-security balance into normative issues. This dilemma is a part of a larger debate on the principles of necessity and proportionality in law, where the actions of the state should be explained by the fact that they are absolutely necessary (McMahan, 2020).

The ethical and legal issues related to the implementation of technologies related to digital policing are one of the critical issues raised by this research. This problem arises because of the validity of law enforcement actions in cases where there are algorithmic biases, lack of transparency, and unclear regulations, as seen in Table 3. These findings resonate with the new models of governance that emphasize accountability and transparency as important aspects of effective governance (Kikasu & Dorasamy, 2025; Mappisabbi and Yappi, 2024). The absence of clear legal standards governing AI-based policing tools poses a risk of having a regulatory backlash whereby technological possibilities surpass the legal control. This unequal position negatively affects not only the confidence of the population but also makes expresses the doubt that there may be systematic discrimination and misuse of authority.

One of the most important aspects of the debate is connected to the effects of digital policing on the basic rights. The findings show that there is an increasing strain between the increased surveillance powers and the safeguarding of civil rights, especially the right to privacy and due process. Such a strain is representative of a bigger constitutional quandary, where national security issues are usually antithetical to the assurance of the rights of people (Hill, 2020). The ideals of necessity and proportionality come to the fore here, where any violation of rights should be both justified and restricted and controlled (McMahan, 2020). In addition, the emerging practices for digital governance are centered on human rights-based approach, thus ensuring that technological developments do not violate the basic legal guarantees (McGregor and Molnar, 2023).

Based on Table 5, we can observe that there is a high degree of variability in the regulatory frameworks used in various jurisdictions and this further depicts absence of a consistent international approach. Although EU approach is more inclined towards safeguarding of human rights by its GDPR guidelines, the US system is quite loose in nature since it is disintegrated. With India, this is an emerging regulatory framework, and this is where the dilemma of the newly-developed laws attempting to cope with the swift technological changes emerges. Considering the above-mentioned findings, it may be concluded that the research offers valuable information to the development of a flexible techno-legal system, which integrates legal, technological, and policy strategies. Such an approach requires having high requirements related to the provision of basic freedoms and being flexible with regard to regulatory rules. The above concept is quite convenient as there is some form of foundation offered by adaptive regulation in reaction to the alteration in technology (Adedoyin and Johnson, 2025). In addition, it is essential to redefine some types of law, including sovereignty and territoriality, regarding the concerns expressed in the paper (Núñez, 2024; Belov, 2021).

In general, there is an immense need to consider further development of legal systems taking into account the complexity of issues associated with cybercrime and online policing. In order to solve problems arising from technological innovations and legal regulation, not only a significant doctrinal change is required but also an interdisciplinary and international strategy should be pursued. Otherwise, the imbalance will remain unchanged, and it will put legal systems under threat.

Conclusion

Besides this, the paper has critically analyzed the legal implications of the relationship between cybercrime and digital policing amidst the rapid emergence of the new technologies. It becomes clear from the results of the research that the current legal system lacks efficiency with regard to

addressing the problems related to jurisdiction, attribution, and digital evidence. Simultaneously, the greater use of technological advancements in the work of law enforcement bodies has caused certain difficulties related to privacy, due process, and accountability. As a consequence, the problem of the growing discrepancy between the demands of security and the protection of basic rights of citizens arises. It is necessary to note the considerable differences between cybercrime regulation and digital policing observed in comparative analysis, which suggests a lack of a universal legal regime. Thus, in order to counterbalance the challenges posed by technological progress, the paper suggests the need for the adoption of flexible and adaptive techno-legal measures. Finally, the study makes a contribution to developing cyber laws by adopting an intermediate stance that would enable striking a balance between the two sides and prevent the existence of an online police force from infringing on the principles of justice and legality.

References

1. Adedoyin, A., & Johnson, I. (2025). Balancing Innovation and Regulation: A Framework for Technology Governance. *ResearchGate [2025]. Disponível em:< www. researchgate. net>. Acesso em*, *12*(06).
2. Afzal, J. (2024). Development of Legal Framework of Digital Laws. In *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (pp. 139-154). Singapore: Springer Nature Singapore.
3. Akpobome, O. (2024). The impact of emerging technologies on legal frameworks: A model for adaptive regulation. *International Journal of Research Publication and Reviews*, *5*(10), 5046-5060.
4. AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28-36.
5. Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews*, *10*(3).
6. Bassini, M. (2019). Fundamental rights and private enforcement in the digital age. *European Law Journal*, *25*(2), 182-197.
7. Belov, M. (2021). Territory, territoriality and territorial politics as public law concepts. In *Territorial Politics and Secession: Constitutional and International Law Dimensions* (pp. 15-43). Cham: Springer International Publishing.
8. Bhatti, N. (2024). Digital Privacy as a Human Rights in the era of Mass Surveillance. *DME Journal of Law*, *5*(02), 120-137.
9. Chatinakrob, T. (2024). Interplay of international law and cyberspace: state sovereignty violation, extraterritorial effects, and the paradigm of cyber sovereignty. *Chinese Journal of International Law*, *23*(1), 25-72.
10. Hill, K. J. (2020). *Balancing national security and the Constitution: The security blanket over civil liberties* (Doctoral dissertation, Johns Hopkins University).
11. Kikasu, E. T., & Dorasamy, N. (2025). Promoting Accountability and Transparency to Ensure Effective Governance. In *Development in Post-Apartheid South Africa* (pp. 103-130). Routledge.
12. Mappisabbi, F., & Yappi, S. T. I. A. (2024). Strengthening transparency and accountability in bureaucracy to enhance public trust. *International Journal of Entrepreneurship and Management*, *1*(4), 101-112.
13. McGregor, L., & Molnar, P. (2023). Digital Border Governance: A human rights based approach.
14. McMahan, J. (2020). Necessity and proportionality in morality and law. *Necessity and Proportionality in International Peace and Security Law*, 3-38.
15. Meghana, G. V. S., Afroz, S. S., Gurindapalli, R., Katari, S., & Swetha, K. (2024, May). A Survey paper on Understanding the Rise of AI-driven Cyber Crime and Strategies for Proactive Digital Defenders. In *2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN)* (pp. 25-30). IEEE.
16. Montasari, R. (2023). The application of big data predictive analytics and surveillance technologies in the field of policing. In *countering cyberterrorism: the confluence of artificial intelligence, cyber forensics and digital policing in US and UK National Cybersecurity* (pp. 81-114). Cham: Springer International Publishing.
17. Mugamba, E. (2025). Global Data Governance in Digital Law: A Comparative Analysis of EU and Global Approaches to Cybersecurity Legislation. Journal of Smart Computing and Quantum Technologies, 1(1), 1-19.
18. Muhammad, R. N., Sutrisno, A., & Mutalib, A. (2025, December). Harmonization of International Trade Law and Criminal Law Regulations for Handling Cybercrime in the Digital Economy Era. In *7th Open Society Conference 2025 (OSC 2025)* (pp. 96-107). Atlantis Press.

19. Núñez, J. E. (2024). State sovereignty: Concept and conceptions. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *37*(7), 2131-2150.
20. Pandey, A. K. (2023). The role of technology in modernizing criminal law: Addressing cybercrime and digital evidence.
21. Place, N. (2018). Double due process: how police unions and law enforcement bills of rights enable police violence and prevent accountability. *USFL Rev.*, *52*, 275.
22. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7-34.
23. Saxena, N., & Mayank, V. (2020). Forensic Hurdles in Investigating & Prosecuting Cyber-crime-An Overview. *The Indian Police Journal*, *67*, 96-110.
24. Tsagourias, N. (2021). The legal status of cyberspace: sovereignty redux?. In *Research Handbook on International Law and Cyberspace* (pp. 9-31). Edward Elgar Publishing.