International Insurance Law Review
ISSN: 0968-2090
Vol 34 S1 (2026): Special Issue
https://lumarpub.com/iilr

Digital Arrest in the Cyber World: Legal Challenges and the Quest for Justice

Akshay Jain[1]
Assistant Professor of Law
IILM School of Law, IILM University, Gurugram, Haryana.
EMAIL ID- akshay.jain@iilm.edu
Jainendra Kumar Sharma[2]
Assistant Professor of Law
IILM School of Law, IILM University, Gurugram, Haryana.
EMAIL ID- jainendra.sharma@iilm.edu

Abstract

In the digital age, the rise of cybercrime has posed significant challenges for law enforcement and the legal framework in India, the concept of digital arrest, defined as the apprehension of individuals suspected of cyber offenses through digital means and the inadequacies of existing legal provisions under the Information Technology Act, 2000, and the Bhartiya Naya Sanhita, 2023, in addressing the convolutions of cybercrime, the critical role of law enforcement agencies in combatting these offenses, emphasising the need for capacity building and inter-agency collaboration. It advocates for wide-ranging legislative reforms, enhanced public awareness, and a balanced approach to ensure justice while protecting individual rights, this seeks to contribute to the ongoing discourse on legal challenges in the cyber territory and the quest for justice in an increasingly digitised society.

Keywords: Digital Arrest, Cybercrime, Law Enforcement, Cyber-security, Digital Evidence.

Introduction

The rapid evolution of digital technology has profoundly transformed societal dynamics, particularly impacting law enforcement and the administration of justice. In India, the digital revolution has led to significant internet penetration and a reliance on online platforms, resulting in a marked increase in cybercrime that challenges the legal system. As criminal activities shift to the virtual area,[1] traditional law enforcement paradigms require re-evaluation. Digital arrest-defined as the apprehension of individuals suspected of cyber offenses through digital means-illustrates the complexities of addressing cybercrime, which often transcends geographical boundaries and exploits online anonymity. Law enforcement agencies grapple with various challenges, including jurisdictional ambiguities and the preservation of digital evidence.[2] This discourse imposes a critical scrutiny of the efficacy of existing legal instruments in India, notably the Information Technology Act, 2000, and the Bhartiya Naya Sanhita, 2023. While these frameworks provide a basis for prosecuting cybercrime, they often fall short in addressing the

[1] D. Chawla and S. Anand, "Cyber Crime and Cyber Security: An Overview," Indian Journal of Science and Technology 8 (2015).

[2] J. P. Kesan and R. Shah, "The Law and Economics of Cybersecurity: A Review of the Literature," University of Illinois Law Review 103 (2005).

Citation: Jain, A; Sharma, J.K. (2026). Digital Arrest in the Cyber World: Legal Challenges and the Quest for Justice. International Insurance Law Review, 34(S1), 285-297.

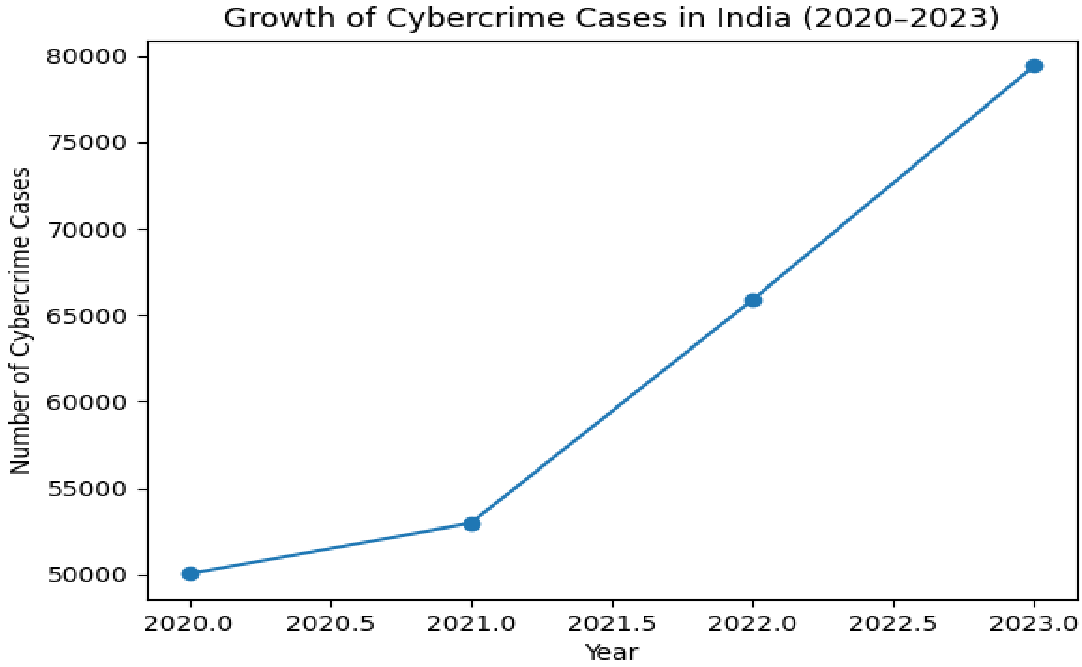
evolving nature of digital offenses.[3] As well, the balance between individual rights and state security raises ethical considerations that require careful navigation.

Table 1: Year-wise Cybercrime Cases Registered in India

Year	Number of Cybercrime Cases
2020	**50,035**
2021	**52,974**
2022	**65,893**
2023	**79,420**

Source: NCRB, *Crime in India* Reports (2020-2023)

Figure-1 *Growth of Cybercrime Cases in India (2020-2023)*



Source: *National Crime Records Bureau (NCRB), Crime in India Reports (2020-2023), Ministry of Home Affairs.*

Understanding Digital Arrest

Digital arrest is a modern legal phenomenon that merges technology with law enforcement to combat cybercrime. It involves apprehending individuals suspected of cyber offenses through

[3] R. Kumar, "Cybercrime in India: An Analysis," 9 International Journal of Cyber Criminology 63 (2015).

digital means, replacing or supplementing traditional arrest methods.[4] Unlike conventional crimes, which involve physical evidence, cybercrimes occur virtually, often spanning multiple jurisdictions and exploiting digital anonymity.[5] This unique aspect needs a re-evaluation of legal definitions, procedural frameworks, and enforcement mechanisms related to arrest. Digital arrest extends beyond mere apprehension; it encompasses the investigative processes used by law enforcement to identify, track, and collect evidence against cybercriminals.[6] Investigations often depend on digital footprints-such as IP addresses, email metadata, and online transactions-that are crucial for understanding a perpetrator's identity and methods. However, reliance on digital evidence raises questions about its integrity, admissibility, and collection methods.[7] Thus, a wide-ranging understanding of digital arrest requires probing the legal principles governing digital evidence, procedural safeguards for individual rights, and the challenges inherent in its application.[8]

Table 2: Arrests and Convictions in Cybercrime Cases (2022)

Indicator	Number
Total Cases Registered	**65,893**
Persons Arrested	**29,155**
Cases Resulting in Conviction	**3,121**
Conviction Rate	**4.7%**

Source: NCRB, *Crime in India 2022*

Table 3: Offence-wise Distribution of Cybercrime (2022)

Type of Offence	Percentage Share
Online Financial Fraud	**64%**
Identity Theft	**12%**
Cyber Harassment	**10%**
Data Breach & Hacking	**8%**
Other Offences	**6%**

[4] R. Anderson and T. Moore, "The Economics of Information Security," 12 Science and Engineering Ethics 231 (2006).

[5] A. Bada and M. A. Sasse, "Cyber Security Awareness Campaigns: Why Do They Fail?" in 10th International Conference on Availability, Reliability and Security, 1-10 (2015).

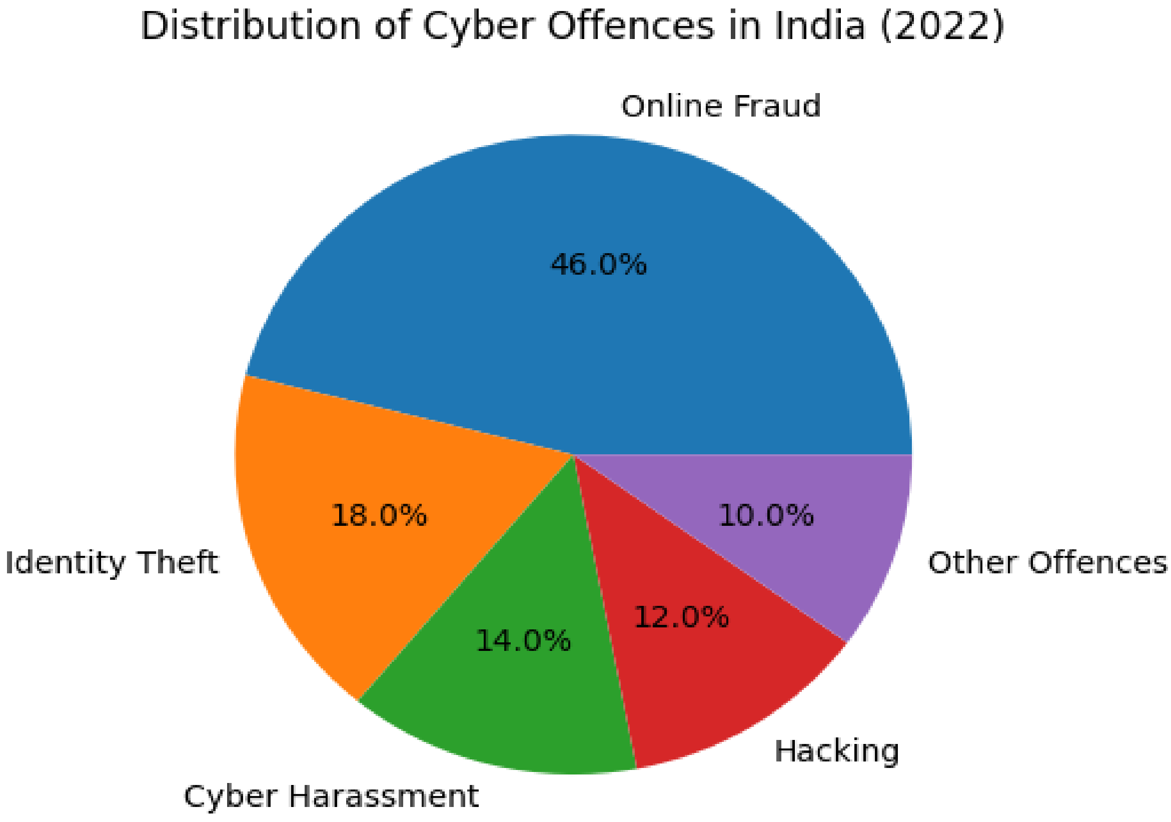
[6] J. P. Barlow, "A Declaration of the Independence of Cyberspace," (1996), *available at:* https://www.eff.org/cyberspace-independence (last visited on Sept. 24, 2024).

[7] I. Brown, "The Need for a New Legal Framework for Cybercrime," 30 Computer Law & Security Review 229 (2014).

[8] M. D. Cavelty, "Cyber Security Meets the Law: The Importance of Regulation," 6 International Journal of Cyber Criminology 811 (2012).

Source: NCRB & I4C Data

Figure -2 *Nature of Cyber Offences in India (2022)*



***Source:** NCRB, Crime in India 2022, Ministry of Home Affairs.*

***Figure 2** depicts the proportional distribution of cyber offences reported in India in 2022. Online financial fraud constitutes the largest category, followed by identity theft and cyber harassment, highlighting the changing character of cybercriminal activity and the increasing reliance on digital arrest mechanisms.*

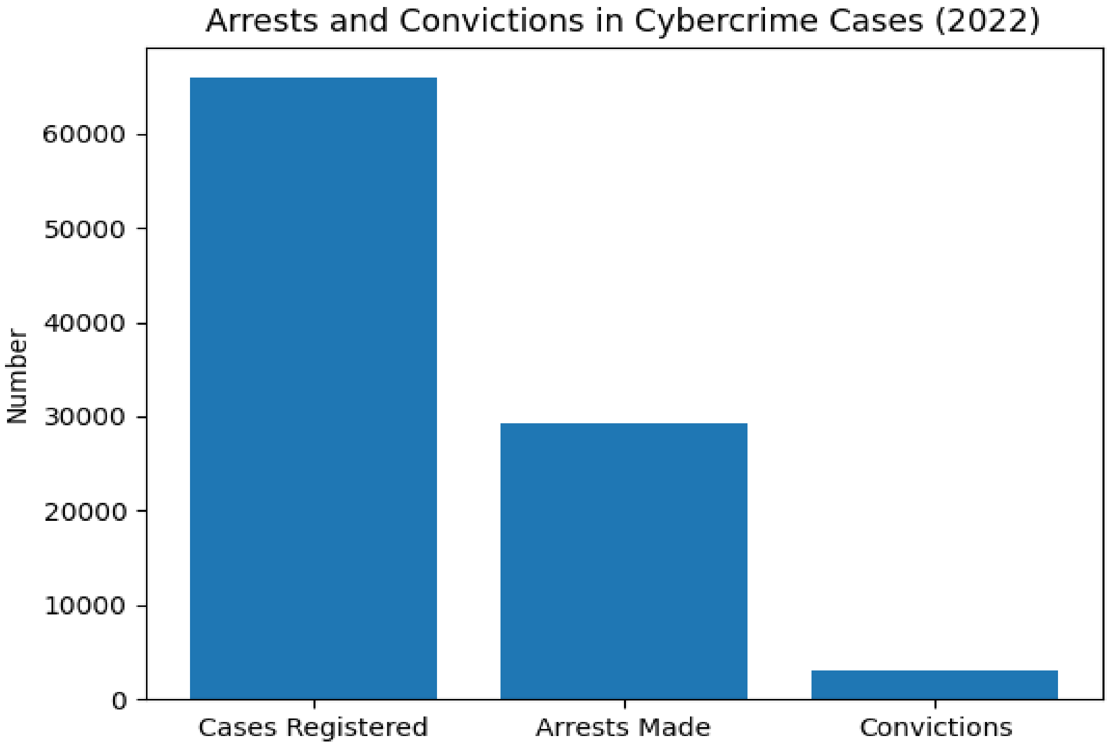
The Evolution of Cybercrime

The rapid evolution of cybercrime parallels advancements in technology and the increasing reliance on digital platforms for personal and commercial interactions. From early hacking and viruses to sophisticated schemes like ransomware and identity theft, the spectrum of cyber offenses has expanded significantly.[9] Cybercriminals employ tactics such as phishing, social engineering, and exploit kits, resulting in substantial financial losses and reputational damage. This convolution is heightened by the internet's global nature, allowing criminals to operate from virtually anywhere, complicating jurisdictional challenges for law enforcement.[10] Traditional legal frameworks designed for the physical world struggle to address the mechanisms of a borderless cyber landscape. Prosecuting cybercrime requires international collaboration, as

[9] R. J. Deibert and R. Rohozinski, "Cyberspace under Siege: A New Framework for International Security" (2010).
[10] L. DeNardis, "The Global War for Internet Governance" (New Haven: Yale University Press, 2014).

effective law enforcement often hinges on cooperation among nations.[11] The dynamic nature of cybercrime accentuates the need for a robust legal framework that addresses current threats and anticipates future developments. As cybercriminals become more sophisticated, law enforcement agencies must adapt their strategies and tools, leveraging technology for digital investigations, enhancing forensic capabilities, and developing legal instruments for timely and effective responses to cyber threats.[12]

Figure 3: *Cybercrime Cases, Arrests, and Convictions (2022)*

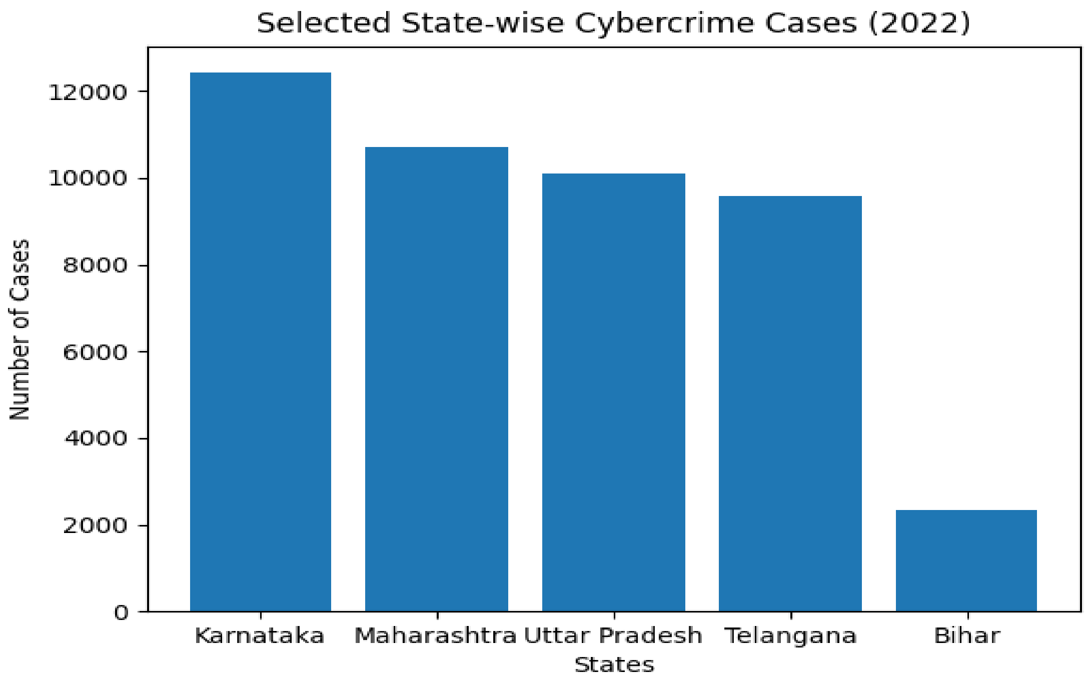


Source: NCRB, Crime in India 2022.

[11] . Goldsmith and T. Wu, "Who Controls the Internet? Illusions of a Borderless World" (New York: Oxford University Press, 2006).

[12] D. Hall, "Digital Evidence and Electronic Signature Law Review," 6 Digital Evidence and Electronic Signature Law Review 23 (2009).

Figure 4: *Selected State-wise Cybercrime Cases (2022)*



Source: NCRB, Crime in India 2022 (State-wise Data).

Legal Framework Governing Digital Arrest in India

- **The Information Technology Act, 2000-** The Information Technology Act, 2000 (IT Act) is the cornerstone of India's legal framework for addressing cybercrime. Initially aimed at promoting electronic governance and recognising electronic records and digital signatures, the IT Act has been amended to encompass offenses like hacking, identity theft, and data breaches.[13] Sections 66, 66C, and 66E outline specific offenses and penalties, forming a basis for prosecution. However, the Act faces criticism for its limited scope and outdated provisions that do not keep pace with evolving technology and emerging cyber threats. Notably, it lacks clear guidelines on the procedural aspects of digital arrests, particularly concerning the collection and admissibility of digital evidence, raising concerns about the rights of suspects and the protection of individual liberties during this process.[14]
- **The Bhartiya Naya Sanhita, 2023-** In response to the evolving landscape of cybercrime, the Indian legislature introduced the Bhartiya Naya Sanhita, 2023 (BNS), aimed at consolidating and updating various criminal laws relevant to cyber offenses. This legislation recognises the need for a coherent framework to address the complexities of

[13] A. Yadav, "Cyber Security and the Role of Law Enforcement Agencies in India," 10 International Journal of Cyber Criminology 45-60 (2016).

[14] R. Henson, "Cybercrime: A New Frontier for Law Enforcement," 1 Journal of Police Studies 45 (2014).

digital arrests.[15] The BNS includes enhanced definitions of cybercrimes and clearer guidelines for handling digital evidence, strengthening the legal framework for digital arrests and equipping law enforcement agencies to combat cybercrime effectively. As well, it emphasises protecting individual rights during investigations, seeking to balance security imperatives with civil liberties.[16]

Statutory Framework Governing Digital Arrests

Law	Provision	Nature of Offence
IT Act, 2000	**s. 66C**	**Identity Theft**
IT Act, 2000	**s. 66D**	**Online Cheating**
BNS, 2023	**s. 318**	**Cheating**
BNS, 2023	**s. 303**	**Criminal Breach of Trust**
CrPC / BNSS	**Arrest Procedures**	**Procedural Safeguards**

Table 4: Complaints Received vs. FIRs Registered (2021-2023)

Year	Complaints Received	FIRs Registered
2021	**14.07 lakh**	**52,974**
2022	**19.02 lakh**	**65,893**
2023	**22.45 lakh**	**79,420**

Source: I4C & NCRB Reports

Challenges in the Legal Framework

The legal framework governing digital arrests in India, while evolving, faces several significant challenges that impede its effectiveness in combating cybercrime. These challenges are rooted in the complexities of the digital landscape, the rapid pace of technological advancement, and the need for a balanced approach to justice and individual rights.[17] Understanding these challenges is

[15] Ravi Sharma, "Navigating Cyber-security in India: Challenges and Solutions," 12 Indian Journal of Cyber Law 45 (2024).

[16] Rajesh Mehta, "Cyber Crime in the Digital Age: An Indian Perspective," 4 Indian Journal of Information Technology Law 89 (2024).

[17] T. J. Holt and A. M. Bossler, "Theoretical Explanations for Cybercrime: A Review of the Literature," 36 Journal of Criminal Justice 176 (2008).

essential for identifying areas requiring reform and for fostering a legal environment conducive to effective law enforcement:

- **Jurisdictional Ambiguities-** A significant challenge in addressing cybercrime is jurisdiction. The digital nature of these offenses allows perpetrators to operate across multiple jurisdictions, often from outside India,[18] complicating prosecution efforts. Existing legal provisions frequently do not address the transnational aspects of cybercrime, leading to ambiguities that hinder timely action. When offenses originate in foreign territories, Indian law enforcement faces hurdles[19] in securing international cooperation. The absence of standardised international legal frameworks results in inconsistencies in how jurisdictions handle cybercrime investigations and prosecutions, which can severely undermine the effectiveness of digital arrests.[20]
- **Admissibility and Integrity of Digital Evidence-** The reliance on digital evidence in cybercrime investigations poses challenges, particularly regarding its admissibility in court. While the integrity of this evidence is crucial, unclear protocols for its collection, preservation, and presentation can compromise its validity.[21] As well, the rapid evolution of technology complicates matters; as cybercriminals become more sophisticated, law enforcement must adapt, but legal standards often lag behind, leading to outdated procedures. This disconnect undermines prosecutions and makes securing convictions difficult.[22]
- **Balancing Security and Individual Rights-** The pursuit of justice in cybercrime requires balancing state security and individual rights. As law enforcement intensifies its efforts, concerns about civil liberties grow, particularly regarding broad surveillance measures and digital arrests that may infringe on privacy rights.[23] Striking this balance is crucial and requires careful consideration. Legislative reforms should include robust safeguards to protect the rights of suspects, ensuring adherence to due process, transparency, and accountability to maintain public trust in the legal system.[24]
- **Evolving Nature of Cybercrime-** The rapid evolution of cybercrime poses a significant challenge to the legal framework for digital arrests. Cybercriminals continuously adapt their tactics to evade detection, compelling a proactive legal framework that responds to these emerging threats.[25] Lawmakers must be vigilant in updating existing laws and

[18] Priya Nair, "Balancing Privacy and Security: The Ethical Implications of Surveillance Technologies," 9 Journal of Indian Law and Technology 67 (2024).
[19] S. Iyer, "Cyber Crime in India: An Overview," 1 Journal of Cyber Security Technology 1 (2016).
[20] J. P. Kesan and R. Shah, "The Law and Economics of Cybersecurity: A Review of the Literature," 2005 University of Illinois Law Review 103 (2005).
[21] M. King, "Cybercrime and Its Legal Challenges: An Overview," 1 Journal of Law and Cyber Warfare 113 (2016).
[22] J. A. Lewis, "Cybersecurity and Cybercrime: An Overview," Harvard Kennedy School Belfer Center for Science and International Affairs, 2014.
[23] A. Moore, "Cyber Crime and Cyber Terrorism: A Real and Present Danger," 21 Computer Law & Security Review 27 (2005).
[24] H. Nissenbaum, "Privacy in Context: Technology, Policy, and the Integrity of Social Life" (Stanford: Stanford University Press, 2010).
[25] A. O'Connell, "Cyber Crime and the Role of Law Enforcement," 6 Journal of Digital Forensics, Security and Law 7 (2011).

enacting new provisions to address evolving challenges. Without this responsiveness, the legal framework may become inadequate, undermining the effectiveness of digital arrests and the pursuit of justice.[26]

The Role of Law Enforcement Agencies

Law enforcement agencies play a pivotal role in the prevention, investigation, and prosecution of cybercrime within the framework of digital arrests. As custodians of public safety and enforcers of the law, these agencies are tasked with circumnavigating the complications of a rapidly evolving digital landscape.[27] Their effectiveness in combating cyber offenses is contingent upon their ability to adapt to technological advancements, implement robust investigative practices, and engage in collaborative efforts both domestically and internationally.[28] This section delineates the multidimensional responsibilities of law enforcement agencies in the context of digital arrests, emphasising their critical role in ensuring justice while safeguarding individual rights.[29]

Preventive Measures- Preventing cybercrime is a key responsibility of law enforcement agencies. In today's digital era, proactive measures are essential to mitigate risks and deter offenders. Agencies enhance public awareness of cyber threats through community outreach, educational campaigns, and collaboration with the private sector.[30] Partnerships with technology companies help develop and implement cyber-security measures, allowing law enforcement to leverage expertise and resources. These collaborations facilitate information sharing on emerging threats, enabling timely responses to prevent cyber offenses.[31]

Investigation and Evidence Collection- The investigative role of law enforcement agencies is vital for digital arrests. Cybercrime investigations require specialised skills in digital forensics to ensure the integrity and admissibility of evidence.[32] Agencies often create dedicated cybercrime units staffed with personnel trained in advanced forensic technologies. These units conduct thorough investigations,[33] including tracing digital footprints, analysing network traffic, and recovering deleted data. Their technical expertise is crucial for building strong cases against cybercriminals and securing successful prosecutions.[34]

[26] J. Porrata, "Understanding Cyber Crime: A Global Perspective," 7 International Journal of Cyber Criminology 25 (2013).

[27] K. Raghu, "Cybercrime in India: Emerging Trends and Issues," 5 Indian Journal of Computer Science and Engineering 192 (2014).

[28] S. Reimer, "Cyber Crime and Cyber Security: An Overview," 3 International Journal of Law and Cyber Warfare 17 (2014).

[29] M. K. Rogers, "A Study of Cyber Crime and Criminal Justice System: An Empirical Analysis," 2 Journal of Criminal Justice Research 101 (2011).

[30] M. N. Schmitt, "Cyber Operations and the Law of Armed Conflict," 4 Harvard National Security Journal 112 (2013).

[31] H. G. Simon, "The Role of Digital Evidence in the Prosecution of Cybercrime," 18 International Journal of Evidence and Proof 246 (2014).

[32] R. G. Smith, "The Impact of Cyber Crime on the Economy," 2 Cybersecurity Review 30 (2015).

[33] Swati Singh, "Data Localization in India: A Critical Assessment of the Personal Data Protection Bill, 2019," 62 Journal of Indian Law Institute 127 (2020).

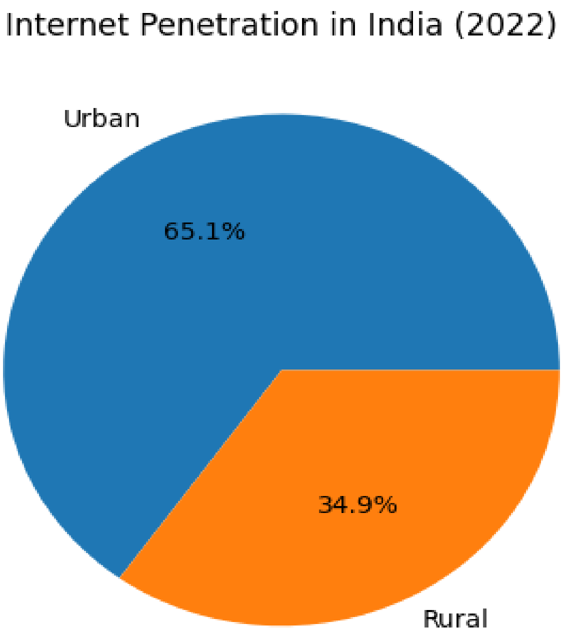
[34] L. Sweeney, "Reputation in the Digital Age: The Role of Trust in Cybersecurity," 1 Journal of Cyber Policy 11 (2016).

Table 5: Internet Penetration in India (2022)

Area	Internet Penetration
Urban	**69%**
Rural	**37%**

Source: TRAI, *Telecom Performance Indicators 2022*

Figure 5: ***Internet Penetration in India: Urban vs. Rural (2022)***



Source: TRAI, Telecom Services Performance Indicators 2021-22; MeitY, Digital India Reports.

Interagency Collaboration- The transnational nature of cybercrime requires collaboration among law enforcement agencies for effective investigation and prosecution. Cybercriminals exploit jurisdictional ambiguities to evade detection, making interagency cooperation essential both domestically and internationally.[35] In India, collaboration among Cyber Crime Cells, the Central Bureau of Investigation (CBI), and local law enforcement is crucial for sharing intelligence

[35] Rajesh Mehta, "Cyber Crime in the Digital Age: An Indian Perspective," 4 Indian Journal of Information Technology Law 89 (2024).

and resources.[36] Internationally, agencies engage in joint task forces, information-sharing networks, and agreements like the Budapest Convention on Cybercrime, facilitating timely information exchanges and coordinated responses to transnational offenses. This enhances law enforcement's effectiveness in combating cybercrime.[37]

Upholding Individual Rights- While law enforcement agencies aim to ensure public safety and prosecute cybercriminals, they must also uphold individual rights during investigations. Digital arrests raise concerns about privacy, surveillance, and potential abuses of power.[38] Agencies should adhere to due process principles, ensuring that suspects' rights are respected by obtaining appropriate warrants, maintaining transparency, and informing individuals of their rights. By upholding these rights, law enforcement not only fosters public trust in the legal system but also demonstrates a commitment to ethical practices.[39]

The Quest for Justice in the Digital Age

The digital age has profoundly transformed the landscape of human interaction, commerce, and governance. While the technological revolution offers unprecedented opportunities for connectivity and innovation, it has also birthed a myriad of challenges that complicate the pursuit of justice.[40] As cybercrime proliferates and digital transactions become the norm, the quest for justice in this new environment necessitates a revaluation of existing legal frameworks, law enforcement strategies, and societal norms. This segment reconnoitres the elaborate relationship between justice and the digital age, highlighting the multidimensional challenges and the imperative for adaptive solutions that safeguard both public safety and individual rights.[41]

- **The Role of Technology in Justice Delivery-** The digital age presents both opportunities and challenges for justice delivery. Innovations like artificial intelligence (AI) and blockchain can improve the efficiency and transparency of judicial processes, with AI aiding in data analysis and blockchain securing transactions.[42] However, reliance on technology raises ethical concerns, as surveillance and algorithm-driven decisions can infringe on privacy rights and introduce biases. It is crucial to balance leveraging technology with safeguarding fundamental rights. Policymakers and stakeholders must engage in dialogue to establish ethical guidelines for technology use in law enforcement and judicial processes.
- **Access to Justice in the Digital Dominion-** Access to justice is a fundamental principle of the rule of law, but the digital age creates unique barriers. Digital divides, stemming from disparities in technology access and literacy, proliferation of inequalities in the

[36] Priya Nair, "Balancing Privacy and Security: The Ethical Implications of Surveillance Technologies," 9 Journal of Indian Law and Technology 67 (2024).
[37] Vikram Singh, "Evolving Legal Frameworks for Cybercrime in India," 25 Journal of Indian Law 133 (2024).
[38] Anjali Verma, "The Role of Artificial Intelligence in Enhancing Cybersecurity Measures," 3 Journal of Indian Cyber Security Law 27 (2024).
[39] Ravi Sharma, "Navigating Cybersecurity in India: Challenges and Solutions," 12 Indian Journal of Cyber Law 45 (2024).
[40] S. Reimer, "Cyber Crime and Cyber Security: An Overview," 3 International Journal of Law and Cyber Warfare 17 (2014).
[41] A. K. Srivastava, "Data Protection and Privacy Concerns in India: A Critical Analysis of the Personal Data Protection Bill," 65 Journal of Indian Law Institute 98 (2023).
[42] Deepak Verma, "Blockchain Technology and Its Legal Implications in the Indian Legal Framework," 24 Indian Journal of Law and Technology 77 (2021).

justice system, particularly for marginalised communities.[43] To improve access to justice, initiatives should focus on promoting digital literacy, enhancing technology access, and ensuring legal resources are user-friendly. Empowering individuals with the necessary tools and knowledge can foster greater equity in pursuing justice.[44]

- **The Ethical Imperative for Justice-** In the quest for justice in the digital age, ethical considerations must be paramount. Rapid technological advancements can lead to abuses of power and violations of individual rights. Law enforcement, legal practitioners, and policymakers should prioritise ethical principles accentuating transparency, [45] accountability, and human rights. Public engagement is crucial for shaping the ethical frameworks governing technology and justice. By incorporating diverse voices in these discussions, society can foster a nuanced understanding of justice that reflects the complexities of the digital era.[46]

Recommendations for Reform

As India navigates the convolutions of the digital age and confronts the challenges posed by cybercrime, it becomes imperative to implement wide-ranging reforms that enhance the efficacy of legal frameworks, law enforcement capabilities, and public engagement. The following recommendations aim to address the gaps in the current system and promote a more robust and equitable approach to justice in the context of digital arrests.

- **Establish Specialised Cybercrime Courts-** To enhance the efficiency of legal proceedings involving cyber offenses, the establishment of specialised cybercrime courts is recommended. These courts would be staffed with judges and legal practitioners trained in cyber law and digital forensics, ensuring a more informed and expedited judicial process.
- **Develop Clear Guidelines on Digital Evidence-** The legal framework should incorporate widespread guidelines regarding the collection, preservation, and admissibility of digital evidence. This will ensure that law enforcement agencies follow standardised procedures, thereby safeguarding the integrity of evidence and reducing challenges related to its admissibility in court.
- **Training and Development Programs-** Law enforcement personnel must receive ongoing training in digital forensics, cyber-security principles, and cyber law. Establishing partnerships with academic institutions and private sector experts can facilitate the development of specialised training programs that equip law enforcement agencies with the necessary skills to effectively investigate and prosecute cybercrimes.
- **Foster Interagency Collaboration-** Enhancing cooperation between various law enforcement agencies at local, state, and national levels is essential. Establishing formal

[43] Meera Menon, "Digital Justice: The Impact of Artificial Intelligence in Indian Judicial Systems," 37 Indian Journal of Law & Technology 155 (2022).

[44] Shashank Shekhar, "Cybercrime Jurisdiction in India: Issues and Challenges," 44 Indian Journal of International Law 213 (2023).

[45] Sunil Reddy, "Blockchain and the Future of Digital Governance in India," 29 Indian Journal of Law and Technology 101 (2022).

[46] Priyanka Sharma, "Cybersecurity Framework in India: Bridging the Gap between Policy and Implementation," 14 Indian Journal of Cyber Law 78 (2023).

mechanisms for information sharing and joint task forces can improve the efficiency and effectiveness of investigations, particularly in complex cases involving transnational cyber offenses.

- **Conduct Impact Assessments-** Prior to the implementation of new technologies in law enforcement, impact assessments should be conducted to evaluate potential implications for privacy rights, discrimination, and social equity. Such assessments can inform policy decisions and help mitigate potential risks associated with technological innovations.

Conclusion

The quest for justice in the digital age presents an innumerable interplay of challenges and opportunities that impose a robust and adaptive legal framework. As cybercrime evolves in sophistication and scope, it is overbearing for India to undertake inclusive reforms that address the limitations of existing laws, enhance law enforcement capacities, and promote public awareness. The establishment of specialised cybercrime units, the implementation of rigorous training programs, and the fostering of interagency collaboration are vital steps toward effective enforcement. Besides, the ethical use of technology must be prioritised to safeguard individual rights while ensuring public safety. Initiatives aimed at enhancing access to justice, particularly for marginalised communities, are essential for creating an equitable legal environment. Ultimately, the effective pursuit of justice in the digital domain requires a collective commitment from policymakers, law enforcement agencies, and society at large to adapt to the realities of a rapidly changing technological landscape. By embracing these reforms, India can foster a legal framework that not only combats cybercrime but also upholds the principles of justice and human rights in an increasingly interconnected world.