INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER CRIME IN THE DIGITAL ECONOMY

AUTHORED BY - UTSHAV SHANKAR PATHAK
AMITY LAW SCHOOL PATNA

ABSTRACT

The digital economy has altered the way individuals communicate, businesses operate, financial services are delivered and public administration is carried out. Online banking, electronic payments, e-commerce, cloud computing, social media and artificial intelligence have created opportunities for innovation and economic inclusion. At the same time, the growing dependence on connected systems has increased exposure to cybercrime. Activities such as phishing, identity theft, unauthorised access, malware distribution, ransomware, online payment fraud, cyberstalking and data theft can cause financial loss, compromise privacy and disrupt essential services. The consequences extend beyond individual victims: businesses may suffer operational interruption and reputational damage, while public institutions and critical infrastructure may face risks to continuity and security. This article examines the meaning and development of cybercrime, its principal forms, the factors contributing to its growth and its economic and social effects. It then considers the Indian legal framework, particularly the Information Technology Act, 2000, relevant provisions of the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023. The article also considers the opportunities and risks associated with artificial intelligence. It argues that effective prevention requires more than criminal penalties: it depends on secure technology, responsible data practices, effective investigation, institutional cooperation and public awareness.

Keywords: Cybercrime; Digital Economy; Cybersecurity; Information Technology Act, 2000; Digital Payments; Data Protection; Artificial Intelligence; Digital India.

1. INTRODUCTION

The digital economy has become an important part of modern economic and social life. Individuals use digital platforms to make payments, obtain public services, communicate, study, shop and conduct business. Organisations rely on electronic records, cloud-based applications, online payment gateways and interconnected networks to manage their

ISSN: 2582-6433

operations. These developments have reduced transaction costs and made services more accessible. They have also increased the volume of personal, financial and commercial information stored or transmitted through digital systems.

Information has economic value, and that value can attract unlawful activity. A compromised bank credential may be used to initiate unauthorised transactions; a stolen customer database may be sold or used for extortion; and an attack on a business network may interrupt services and damage commercial confidence. Cybercrime therefore affects more than the immediate victim. It can undermine trust in online markets, increase the cost of doing business and weaken confidence in digital public infrastructure.

In India, the expansion of Digital India services, Unified Payments Interface (UPI), mobile banking and e-commerce has made digital transactions familiar to a growing section of the population. The convenience of these services must be accompanied by safeguards. Users need reliable information and secure platforms, while organisations must protect systems and respond appropriately to incidents. Law-enforcement agencies also require technical capacity and timely access to admissible electronic evidence. Cybercrime is consequently a legal, economic, technological and social concern rather than a purely technical problem.

This article studies cybercrime in the context of the digital economy. It explains the concept and development of cybercrime, identifies common forms and causes, examines its effects, and discusses the principal Indian laws relevant to prevention, investigation and accountability. It also considers how artificial intelligence may be misused as well as employed in cyber defence.

2. MEANING AND CONCEPT OF CYBERCRIME IN THE DIGITAL ECONOMY

Cybercrime is commonly used to describe unlawful conduct in which a computer, computer system, communication network or digital data is the target, the instrument or an important part of the offence. Some offences are directed against computer resources themselves, such as unauthorised access, interference with data or disruption of a network. Other offences use digital technology as a means of committing conduct that may also occur offline, including cheating, impersonation, extortion, harassment or the circulation of unlawful material.

The digital economy refers broadly to economic activity that depends on digital technologies, data, online networks and electronic services. It includes digital banking, e-

ISSN: 2582-6433

commerce, electronic payment systems, online education, digital marketing, software services, cloud-based business operations and technology-enabled financial services. These activities depend on the collection, processing, storage and transfer of information. The same dependence creates vulnerabilities when systems are poorly secured or when users are manipulated into disclosing credentials.

Cybercrime differs from many traditional offences because the offender, victim, device, server and financial destination may be located in different places. A person operating from one jurisdiction may compromise a system in another, while the proceeds may pass through several accounts or payment services. Digital evidence can also be altered, deleted or moved quickly. These features create practical challenges for identifying suspects, preserving evidence and coordinating investigations across borders.

3. HISTORICAL DEVELOPMENT OF CYBERCRIME

The development of cybercrime has followed the expansion of computing and communication technology. In the early stages of computerisation, access to computers was concentrated in government bodies, research institutions and large organisations. Misuse largely involved unauthorised access, manipulation of programs or interference with stored information. As personal computers became widely available, the number of potential targets increased and malicious software became more accessible.

The growth of the internet connected users and organisations across national boundaries. Electronic commerce and online banking made it possible to conduct transactions without physical contact, but they also created opportunities for credential theft, fraudulent websites and deceptive electronic communications. The spread of smartphones and social media added further risks, including account takeovers, impersonation, cyberbullying, stalking and the non-consensual circulation of private material.

In India, the Information Technology Act, 2000 marked a major legislative step. It recognised electronic records and electronic signatures and created provisions addressing specified forms of misuse of computer resources. Subsequent technological changes have made cybercrime more varied and sophisticated. The development of digital payments, cloud services, artificial intelligence and connected devices means that cybersecurity and cyber law must continue to adapt.

ISSN: 2582-6433

4. MAJOR TYPES OF CYBERCRIME IN THE DIGITAL ECONOMY

4.1 Unauthorised access and hacking

Unauthorised access occurs when a person enters or interferes with a computer resource without permission. Depending on the method and purpose, an intruder may view confidential information, alter records, install malicious software or disrupt normal operations. For a business, a successful intrusion may expose trade secrets, customer information, financial records or internal communications. Attacks on public systems may also affect the delivery of essential services.

4.2 Phishing and social-engineering fraud

Phishing involves deceptive messages, websites or calls designed to persuade a person to reveal confidential information or take an action that benefits the offender. A message may appear to come from a bank, government department, delivery service or familiar business. In India, common themes include requests to update KYC details, verify an account, pay an electricity bill, receive a parcel or claim a refund. Fraudsters often create urgency or fear so that the recipient acts before checking the source. Social engineering is broader than phishing and includes manipulation through calls, messages and other forms of personal interaction.

4.3 Identity theft and online impersonation

Identity theft involves the unauthorised use of another person's identifying information or credentials. Stolen passwords, account details, identification data or electronic-signature credentials may be used to access accounts, create false profiles, obtain services or carry out transactions in another person's name. Victims may face continuing difficulties because they must report the misuse, secure accounts and dispute transactions or records they did not authorise.

4.4 Online banking and digital-payment fraud

Digital-payment fraud may involve fake customer-care numbers, fraudulent payment links, QR-code deception, false payment requests, remote-access applications or impersonation of bank personnel. A common misunderstanding is that scanning any QR code will automatically result in receiving money. In many payment situations, scanning a code or approving a request may instead initiate a payment from the user's account. Users should verify the recipient and transaction details and should never disclose an OTP, PIN or password to an unknown person.

ISSN: 2582-6433

4.5 Malware and ransomware

Malware is software designed to damage, disrupt, monitor or gain unauthorised access to a device or system. It includes viruses, worms, spyware, trojans and other malicious programs. Malware may reach a user through infected attachments, unsafe downloads, counterfeit applications or compromised websites. Ransomware is a particularly harmful form of attack in which data or systems are made inaccessible, often through encryption, and a payment is demanded for restoration or to prevent disclosure of stolen information. Payment does not guarantee recovery of data.

4.6 Cyberstalking, harassment and privacy violations

Digital communication tools may be misused to threaten, monitor, intimidate or repeatedly harass individuals. Conduct may include threatening messages, fake profiles, publication of private information, non-consensual sharing of intimate images or coordinated online abuse. Such conduct can affect personal safety, dignity, reputation and mental well-being. Reporting mechanisms and sensitive support for victims are important parts of an effective response.

4.7 Data theft and cyber extortion

Data theft occurs when confidential information is obtained or copied without authority. Stolen information may be sold, used for identity fraud, or exploited to gain access to other systems. Cyber extortion involves threats to disclose information, damage systems or otherwise harm a victim unless money or another benefit is provided. Businesses may be targeted through threats involving customer databases, commercial secrets, financial records or internal communications. Organisations should preserve relevant logs and evidence and obtain appropriate technical and legal assistance.

4.8 AI-enabled impersonation and deepfakes

Artificial intelligence tools can generate or manipulate images, audio and video in ways that appear convincing. Criminals may imitate the voice or appearance of a relative, senior employee or public figure to request money, obtain confidential information or spread false claims. Synthetic media can also be used to create targeted phishing messages. The increasing realism of such material makes independent verification, multi-factor authentication and agreed internal approval procedures more important.

ISSN: 2582-6433

5. CAUSES AND FACTORS RESPONSIBLE FOR THE GROWTH OF CYBERCRIME

One important factor is the rapid expansion of internet access and digital services. As more individuals and organisations use smartphones, online banking, electronic payments and cloud platforms, the number of potential targets grows. The speed of digital adoption may exceed the development of users' security awareness. Weak passwords, reused credentials, careless sharing of OTPs and use of unverified links can make it easier for offenders to gain access or manipulate victims.

Limited digital literacy is another significant factor. Fraudsters exploit trust, fear, greed and urgency. Offers of employment, scholarships, investment returns, refunds or prizes may be used to persuade individuals to disclose confidential details or transfer money. A person may also rely on a search result or online number without checking whether it is an official contact channel.

Organisational weaknesses can increase exposure. Outdated software, inadequate access controls, insufficient backups, poor network monitoring and a lack of employee training may create opportunities for attack. Small and medium-sized businesses may face particular difficulties because they have limited budgets and may not employ dedicated cybersecurity professionals. A single compromised device can sometimes provide an entry point into a wider organisational network.

Cybercrime is also supported by the availability of malicious tools and services through illicit online networks. Some offenders operate individually, while others participate in organised groups that specialise in phishing, ransomware, data theft, laundering or the sale of compromised credentials. The cross-border nature of the internet further complicates enforcement because evidence and suspects may be located in different jurisdictions, each with its own legal procedures.

6. IMPACT OF CYBERCRIME ON THE DIGITAL ECONOMY

Financial loss is among the most direct consequences of cybercrime. Individuals may lose savings through fraudulent transfers, while businesses may incur losses from stolen funds, ransom demands, interrupted operations and the cost of restoring systems. Additional expenditure may be required for forensic investigation, legal advice, customer support, regulatory compliance and improved security.

Cyber incidents can damage confidence in digital services. Consumers may become

ISSN: 2582-6433

reluctant to use online banking, make electronic payments or share information with a platform after learning of a serious breach. Businesses may lose customers, commercial partners and investment opportunities if they are unable to demonstrate that information is handled securely. Restoring public confidence after a major incident can take considerable time.

Cyberattacks may also interrupt essential services. Attacks directed at payment networks, hospitals, communications, electricity systems or government platforms can affect large numbers of people. The consequences may extend beyond commercial loss and create risks to public safety and administrative continuity. Protection of critical information infrastructure is therefore an important public responsibility.

The effects are not distributed equally. People with limited digital skills may find it harder to identify scams or obtain assistance after victimisation. Older persons, children, women and first-time users of digital services may face particular forms of online abuse or deception. Small businesses may also struggle to recover from a major incident. Cybercrime can therefore deepen existing economic and digital inequalities.

7. CYBERCRIME IN INDIA: THE DIGITAL TRANSACTION CONTEXT

India's digital economy has expanded through mobile connectivity, online banking, e-commerce, digital public services and UPI-based payments. These services have made transactions faster and more accessible. However, the growth in digital activity has also created opportunities for fraudsters to target users through fake payment requests, impersonated customer-support services, fraudulent links and social-engineering calls.

The technology used for digital payments is not necessarily the source of the fraud. In many cases, offenders manipulate users into authorising a transfer, sharing credentials or installing a remote-access application. Clear user interfaces, effective grievance redressal, rapid reporting channels and cooperation between banks, payment providers and law-enforcement agencies are therefore important.

E-commerce presents related challenges. Consumers may encounter counterfeit sellers, misleading listings, fake websites, non-delivery of goods or deceptive refund processes. Platforms should maintain appropriate seller-verification, complaint-handling and account-moderation processes, while consumers should verify sellers and payment channels before completing transactions. A secure digital economy requires both reliable technology and accountability across the organisations that provide digital services.

ISSN: 2582-6433

8. LEGAL FRAMEWORK GOVERNING CYBERCRIME IN INDIA

India's legal response to cybercrime is spread across legislation dealing with computer resources, general criminal offences, criminal procedure, electronic evidence, data protection and consumer rights. The Information Technology Act, 2000 is the principal statute specifically addressing several forms of computer-related misconduct. It also recognises electronic records and electronic signatures. The provisions applicable to a particular incident depend on the facts and the elements of the alleged offence.

8.1 Information Technology Act, 2000

Section 43 addresses specified unauthorised acts involving computer resources, including unauthorised access, copying or extraction of data, introduction of contaminants and damage or disruption. Where the conduct is carried out dishonestly or fraudulently, Section 66 may make the relevant acts criminal offences. Section 66C concerns identity theft through fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. Section 66D addresses cheating by personation using a communication device or computer resource. Section 66E concerns violation of privacy through capturing, publishing or transmitting images of a person's private area in the circumstances covered by the provision.

Section 66F deals with cyberterrorism. Sections 67, 67A and 67B address specified categories of obscene, sexually explicit and child sexual abuse material in electronic form. Section 70B provides for the Indian Computer Emergency Response Team (CERT-In), which performs national functions relating to cybersecurity incident response, alerts and coordination. The Act should be read with applicable rules, directions and judicial interpretation; not every online dispute automatically amounts to an offence under the Act.

8.2 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) is the general criminal law statute that replaced the Indian Penal Code, subject to its commencement and applicable transitional rules. Its provisions may apply where conduct committed through digital means also constitutes a general offence. Depending on the facts, provisions concerning cheating, cheating by personation, forgery and related conduct may be relevant. The BNS therefore complements the Information Technology Act; it does not replace the need to identify the precise legal ingredients of each alleged offence.

ISSN: 2582-6433

8.3 Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) provides the procedural framework for criminal investigation, inquiry and trial. Its relevance to cybercrime includes the processes through which complaints are recorded, investigations are conducted, evidence is collected and cases proceed before criminal courts. Because electronic evidence can be volatile, investigators must take care to preserve devices, logs, account records and other relevant material in a lawful and reliable manner.

8.4 Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) governs the law of evidence and contains provisions concerning electronic and digital records. In cybercrime proceedings, relevant material may include emails, messages, server logs, call records, transaction records, CCTV footage, device data and digital documents. The authenticity, integrity, source and manner of production of such material may be important to its admissibility and evidentiary value. Investigators and litigants should follow the applicable statutory requirements rather than assume that a screenshot alone will always be sufficient.

8.5 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 establishes a framework for processing digital personal data and sets out obligations for entities processing such data, together with rights and protections for individuals. Its relevance to cyber risk lies in the need for lawful and responsible data handling, appropriate safeguards and accountability in the event of specified data-related incidents. The Act's provisions and the Digital Personal Data Protection Rules, 2025 have commencement arrangements that must be checked against the applicable government notifications. Accordingly, legal analysis should identify which provisions were in force on the date of the relevant conduct instead of assuming that every provision commenced simultaneously.

8.6 Consumer protection and e-commerce regulation

The Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 are relevant where online transactions give rise to consumer complaints, unfair trade practices, misleading representations or failures by e-commerce entities to meet applicable duties. These instruments do not criminalise every cyber incident, but they form part of the wider framework for consumer protection in digital markets. Depending on the facts, a victim

ISSN: 2582-6433

may need to consider consumer remedies alongside criminal or data-protection routes.

8.7 Reporting and institutional response

Users in India can report cybercrime through the National Cyber Crime Reporting Portal and, in urgent financial-fraud situations, should contact the relevant bank or payment provider promptly and use the appropriate national helpline. CERT-In performs national cybersecurity incident-response functions. Effective response depends on prompt reporting, preservation of evidence, cooperation among institutions and clear communication with affected users. The applicable reporting route may vary according to the nature of the incident and the person or organisation affected.

9. CYBERCRIME AND ARTIFICIAL INTELLIGENCE

Artificial intelligence is increasingly used in banking, healthcare, education, manufacturing, telecommunications and business administration. It can process large datasets, identify patterns and support faster decisions. These capabilities can improve cybersecurity, but they can also be misused. AI-generated audio, images and videos may be used to impersonate individuals or create false evidence. A fabricated voice message appearing to come from a family member or senior employee may pressure a recipient into making an urgent payment.

AI tools may also help offenders prepare convincing phishing messages in different languages and tailor them to a particular victim. Automation can increase the scale and speed of malicious activity. These risks do not mean that AI itself is unlawful; rather, they demonstrate the importance of responsible use, reliable authentication and effective safeguards. Organisations should establish independent verification procedures for sensitive payments and changes to financial instructions. Individuals should verify unusual requests through a separate, trusted channel.

At the same time, AI can support defensive cybersecurity. Systems may identify unusual login patterns, flag suspicious transactions, monitor network activity and help security teams prioritise alerts. Human review, data quality, privacy safeguards and accountability remain important because automated systems can produce errors or unfair outcomes. The objective should be to encourage beneficial innovation while reducing the opportunities for misuse.

ISSN: 2582-6433

10. PREVENTION AND RECOMMENDATIONS

First, digital literacy should be strengthened through schools, universities, workplaces and public-awareness programmes. Users should be taught to verify website addresses and caller identities, avoid sharing passwords, PINs and OTPs, use strong and unique passwords, enable multi-factor authentication and install software only from trusted sources. Suspicious payment requests should be checked independently before approval.

Second, organisations should adopt a risk-based cybersecurity programme. Important measures include timely software updates, access controls, encryption where appropriate, regular backups, employee training, network monitoring, incident-response plans and periodic security assessments. Small businesses may benefit from shared expertise, affordable security services and sector-specific guidance.

Third, banks, payment providers, online platforms and telecommunications companies should maintain accessible reporting channels and respond quickly to credible complaints. They should communicate clearly with users, investigate suspicious activity and cooperate with lawful requests from competent authorities. Organisations should also preserve relevant digital records in a manner that protects integrity and supports lawful investigation.

Finally, law-enforcement agencies require continuing training in digital forensics, cryptocurrency tracing, cloud evidence and cross-border cooperation. Legal rules should be applied consistently with due process, privacy and other fundamental rights. A proportionate approach is necessary: cybersecurity measures should protect users without creating unnecessary surveillance or restricting legitimate digital activity.

11. CONCLUSION

Cybercrime has become a serious challenge for the digital economy because individuals, businesses and public institutions increasingly depend on connected systems and electronic information. Phishing, identity theft, unauthorised access, payment fraud, malware, ransomware, data theft, cyberstalking and AI-enabled impersonation can cause financial loss, privacy violations, reputational harm and disruption of essential services. Their effects extend beyond individual victims and may weaken public confidence in digital markets and public infrastructure.

India has developed a legal framework that includes the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Digital Personal Data Protection Act, 2023 and

ISSN: 2582-6433

consumer-protection legislation. These laws address different aspects of digital misconduct, criminal procedure, electronic evidence, data handling and online transactions. Their effectiveness depends on correct application, institutional capacity, timely investigation and awareness among users. The commencement status of relevant provisions and rules must also be checked when advising on a particular incident.

No single measure can eliminate cybercrime. A safer digital economy requires secure systems, responsible data practices, informed users, capable investigators, effective remedies and cooperation between public authorities and private organisations. Digital literacy should be treated as an essential part of education, while cybersecurity should be integrated into business planning and public administration. Ultimately, the success of digital transformation depends not only on technological progress but also on the trust, safety and accountability experienced by those who use it.

REFERENCES

- The Information Technology Act, 2000 (Act No. 21 of 2000), Government of India.
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), Government of India.
- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023), Government of India.
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), Government of India.
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Government of India.
- The Consumer Protection Act, 2019 (Act No. 35 of 2019), Government of India.
- The Consumer Protection (E-Commerce) Rules, 2020, Ministry of Consumer Affairs, Food and Public Distribution, Government of India.
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
- Indian Computer Emergency Response Team (CERT-In), Directions under section 70B of the Information Technology Act, 2000, dated 28 April 2022.
- Ministry of Electronics and Information Technology, Government of India, Digital India programme resources.
- National Cyber Crime Reporting Portal, Government of India.

ISSN: 2582-6433

- Radha Ranjan, 'The Cybersecurity Legal Landscape: Challenges and Opportunities' in Legally Bound: Exploring the Tapestry of Criminal Justice 158–169 (Juris Cognita Publications, 2024).
- Radha Ranjan et al., 'Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches' in Ricardo Marcão, Vasco Ribeiro Santos and Nuno Mateus-Coelho (eds.), Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches 217–264 (IGI Global Scientific Publishing, 2026), DOI: 10.4018/979-8-3373-5992-2.ch007
- Radha Ranjan and Jivantika Gulati, 'The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law' (2023) Vol. 10, No. 1, Kashmir Journal of Legal Studies 79–90, ISSN 2250-2084 (July 2023).
- Bheem Singh Meena, Radha Ranjan and Shyam Kumar Anand, "Virtual Meetings Under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era," 4(2) ShodhKosh: Journal of Visual and Performing Arts 1256–1263 (2023), doi: 10.29121/shodhkosh.v4.i2.2023.3047.
- Radha Ranjan and Pallavi Singh, "Cyber Crime Against Women in Cyber Space: A Critical Analysis of Indian Legislations," 10(1A) Kanpur Philosophers 79–85 (2023).