International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Criminal Liability for Data Breaches Under Indian Law: Need for a Comprehensive Legal Framework

Ankit Singh Gehlot[1], Dr. Gawaraja Suthar[2]

[1]Research Scholar, Department of Law, Apex University, Jaipur (Raj.)
Email: *advankitsinghgehlot[at]gmail.com*

[2]Assistant Professor, Department of Law, Apex University, Jaipur (Raj.)
Email: *gawaraja.suthar[at]apexmail.in*

Abstract: ***The rapid digitalization of Indian society has transformed governance, commerce, communication, and social interaction. However, the increasing dependence on digital technologies has also resulted in growing concerns relating to privacy violations, cyber insecurity, and unauthorized disclosure of personal data. India has witnessed a sharp rise in cybercrimes, including data breaches involving financial institutions, healthcare databases, e-commerce platforms, educational institutions, and government portals. While the Indian legal system addresses certain aspects of cybercrime through statutes such as the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and provisions of the Bharatiya Nyaya Sanhita, 2023, the absence of a comprehensive criminal liability framework for data breaches remains a significant legal challenge. This research paper critically examines the legal dimensions of criminal liability for data breaches in India in alignment with the broader thesis concerning privacy, security, and criminal accountability in Indian digital societies with special reference to Jodhpur. The study analyzes existing statutory provisions, judicial approaches, institutional mechanisms, and comparative international practices. It further explores the limitations of the present legal framework, particularly in relation to corporate accountability, cross-border data breaches, victim compensation, digital evidence, and enforcement challenges. The paper argues that India requires a specialized and comprehensive legal framework that clearly defines criminal liability for negligent and intentional data breaches while balancing innovation, digital governance, and constitutional privacy rights.***

Keywords: Data Breach, Cybercrime, Criminal Liability, Privacy, Digital Security, Information Technology Act, Digital Personal Data Protection Act, Cyber Accountability

1. Introduction

The emergence of digital societies in India has fundamentally altered the manner in which individuals communicate, transact, and access public services. Digital governance initiatives such as Aadhaar-linked services, online banking systems, e-commerce platforms, digital health records, and educational databases have significantly expanded the collection and processing of personal data. While these technological advancements have contributed to economic growth and administrative efficiency, they have simultaneously increased the vulnerability of individuals to cyber threats and data breaches.

A data breach generally refers to unauthorized access, disclosure, theft, alteration, or destruction of personal or sensitive information stored in digital systems. Such breaches may occur due to hacking, phishing attacks, insider misconduct, negligence, malware, ransomware attacks, or inadequate cybersecurity measures. In recent years, India has witnessed several large-scale incidents involving leakage of personal information, financial fraud, identity theft, and unauthorized sale of sensitive data on digital platforms.

The constitutional recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India has strengthened the legal discourse surrounding data protection and digital accountability. However, despite judicial recognition of privacy rights, India still lacks a unified and comprehensive criminal law mechanism specifically dealing with data breaches[1]. Existing laws focus primarily on cyber offenses, unauthorized access, and civil compensation rather than establishing clear criminal accountability for organizations and individuals responsible for negligent data protection practices.

The issue becomes particularly important in rapidly urbanizing regions such as Jodhpur, where digital services are increasingly integrated into public administration, banking, healthcare, education, and law enforcement systems. The growing digital ecosystem in such regions creates new legal challenges concerning cybersecurity preparedness, public awareness, and institutional accountability.

This paper seeks to critically examine whether the current Indian legal framework adequately addresses criminal liability arising from data breaches and whether India requires a more comprehensive and specialized legal framework to protect privacy and ensure accountability in digital societies.

2. Meaning and Nature of Data Breaches

A data breach occurs when confidential, sensitive, or protected information is accessed, disclosed, or used without authorization. Data breaches may involve personal information such as names, addresses, biometric records, financial information, passwords, medical records, and government identification details.

Data breaches may be classified into the following categories:

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

1) **External Cyberattacks** – Unauthorized access by hackers, cybercriminals, or foreign entities.
2) **Insider Threats** – Breaches caused by employees or authorized individuals misusing access privileges.
3) **Negligent Data Handling** – Failure of organizations to adopt reasonable cybersecurity measures.
4) **Accidental Disclosure** – Unintentional exposure of data due to human or technical errors.
5) **Ransomware and Malware Attacks** – Cyberattacks involving encryption or theft of data for extortion.

The consequences of data breaches extend beyond financial loss. Victims may suffer identity theft, reputational damage, psychological distress, surveillance risks, and violation of informational privacy. At a societal level, repeated data breaches weaken public trust in digital governance and technological systems.

Constitutional Dimensions of Privacy and Digital Security

The constitutional foundation for data protection in India emerged prominently through the landmark judgment in Justice K.S. Puttaswamy v. Union of India, wherein the Supreme Court recognized privacy as an intrinsic part of Article 21 of the Constitution of India[2].

The Court observed that informational privacy is an essential aspect of personal liberty in the digital age. It emphasized that the State has a positive obligation to protect citizens' data from unauthorized intrusion. This judgment significantly influenced the development of data protection legislation in India[3].

The constitutional principles relevant to data breaches include:

- Right to privacy
- Right to dignity
- Protection against arbitrary surveillance
- Informational self-determination
- Data autonomy
- Accountability of State and private entities

The constitutional framework therefore imposes a legal and moral obligation upon both public authorities and private corporations to ensure data security and prevent unauthorized disclosure of personal information.

Existing Legal Framework Governing Data Breaches in India

1) Information Technology Act, 2000

The Information Technology Act, 2000 remains the principal legislation dealing with cyber offenses in India. Certain provisions address unauthorized access, hacking, and failure to protect sensitive data.

Section 43A

Section 43A imposes liability upon body corporates that fail to implement reasonable security practices resulting in wrongful loss or gain. However, the provision primarily provides for compensation rather than criminal punishment[4].

Section 66

Section 66 criminalizes dishonest or fraudulent acts involving computer-related offenses such as unauthorized access and data theft[5].

Section 72A

Section 72A penalizes disclosure of personal information in breach of lawful contracts. However, its application remains limited because prosecution requires proof of intentional disclosure and wrongful intent[6].

Limitations

- No comprehensive definition of data breach
- Limited criminal liability for negligence
- Absence of strict corporate accountability
- Weak enforcement mechanisms
- Inadequate victim compensation procedures

2) Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents India's first dedicated data protection legislation. The Act introduces obligations for data fiduciaries regarding lawful processing, consent, data security, and breach notification[7].

Key features include:

- Consent-based data processing
- Rights of data principals
- Obligations of data fiduciaries
- Data breach notification requirements
- Penalties for non-compliance

Despite its significance, the Act largely adopts a regulatory and administrative approach rather than a criminal liability model. Monetary penalties are emphasized over criminal prosecution.

Major Concerns under the Existing Data Protection Framework

One of the primary concerns in the present Indian data protection regime is the lack of detailed criminal sanctions for serious data breaches. Existing laws such as the Digital Personal Data Protection Act, 2023 mainly emphasize monetary penalties and regulatory compliance rather than criminal prosecution. As a result, corporations or individuals responsible for negligent handling of sensitive personal data may escape stringent punishment, even when breaches cause severe harm to citizens. The absence of clear criminal liability weakens deterrence and reduces accountability in the digital ecosystem.

Another significant issue is the broad exemptions granted to government agencies. The legislation permits the State to

[2] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[3] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[4] Information Technology Act, 2000, S 43A, No. 21, Acts of Parliament, 2000 (India).
[5] Information Technology Act, 2000, S 66, No. 21, Acts of Parliament, 2000 (India).
[6] Information Technology Act, 2000, S 72A, No. 21, Acts of Parliament, 2000 (India).
[7] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

exempt certain governmental bodies from compliance requirements on grounds such as national security, public order, and sovereignty. While such exemptions may be necessary in limited circumstances, excessively broad discretionary powers create risks of surveillance, misuse of personal information, and erosion of citizens' privacy rights. This raises concerns regarding transparency and constitutional safeguards under Article 21[8].

The framework also suffers from limited clarity regarding cross-border accountability. Cybercrimes and data breaches frequently involve foreign entities, multinational corporations, or servers located outside India. However, Indian law lacks comprehensive mechanisms for international cooperation, jurisdictional enforcement, and extradition in digital offenses. Consequently, investigation and prosecution become difficult in transnational cybercrime cases.

Further, there are inadequate remedies available to victims of data breaches. Victims often face identity theft, financial fraud, reputational harm, and psychological distress, yet the legal framework provides limited compensation mechanisms and procedural support. The absence of specialized cyber tribunals and simplified grievance redressal systems further restricts access to justice for affected individuals.

3) Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 contains provisions relating to cheating, forgery, identity fraud, and electronic deception which may apply in cases involving misuse of breached data[9].

However, the legislation does not specifically define criminal liability for data breaches caused by negligent cybersecurity practices or systemic failures.

3. Criminal Liability for Data Breaches

Criminal liability arises when a person or organization commits an act prohibited by law with criminal intention, recklessness, fraud, or gross negligence. In the digital era, data breaches have become a major threat to privacy, cybersecurity, and public trust. Personal information such as financial records, biometric data, passwords, medical details, and confidential government information is increasingly stored in digital systems, making it vulnerable to misuse and cyberattacks. Under Indian law, criminal liability for data breaches may arise in several situations, although the present framework remains fragmented and insufficient.

1) Intentional Data Theft

Intentional data theft occurs when individuals or cybercriminals deliberately access, steal, copy, or sell confidential data without authorization. Such acts are usually committed for financial gain, revenge, espionage, blackmail, or malicious purposes. Stolen data may include banking information, Aadhaar details, passwords, trade secrets, or medical records. Cybercriminals often sell such information on illegal digital platforms or use it for identity theft and online fraud. Under the Information Technology Act, 2000, unauthorized access and hacking may attract criminal punishment. However, existing provisions are often inadequate in addressing sophisticated cybercrimes involving organized digital networks and large-scale data trafficking operations.

2) Corporate Negligence

Corporate negligence arises when organizations fail to implement reasonable cybersecurity measures despite foreseeable risks of data breaches. Many companies collect and store massive amounts of personal information but neglect adequate encryption, cybersecurity audits, employee training, or security protocols. Such negligence may expose sensitive customer data to hackers and cybercriminals. Although Section 43A of the Information Technology Act, 2000 provides compensation for failure to protect data, criminal accountability for negligent corporations remains weak. In many cases, corporations avoid liability by treating data protection merely as a compliance requirement rather than a legal obligation. Stronger criminal sanctions are necessary to ensure responsible data management and cybersecurity preparedness.

3) Insider Misconduct

Insider misconduct refers to situations where employees, contractors, or authorized personnel misuse their access privileges to leak, copy, or misuse confidential information. Insider threats are particularly dangerous because authorized persons often have direct access to sensitive databases and security systems. Data may be disclosed for personal profit, revenge, or corporate espionage. In banking, healthcare, and government sectors, insider misconduct can result in severe privacy violations and financial harm. Existing Indian laws criminalize unauthorized disclosure of information in limited circumstances, but enforcement remains difficult. Organizations must therefore adopt strict internal controls, employee monitoring systems, and accountability mechanisms to reduce risks arising from insider abuse of digital access privileges.

4) Failure to Report Breaches

Organizations sometimes intentionally conceal data breaches to avoid reputational damage, regulatory penalties, or financial losses. Failure to report breaches prevents affected individuals from taking protective measures such as changing passwords, monitoring financial transactions, or securing personal accounts. Concealment also delays investigation by regulatory authorities and weakens public trust in digital systems. The Digital Personal Data Protection Act, 2023 introduces obligations regarding breach notification, but the framework still lacks detailed criminal consequences for deliberate non-reporting. A comprehensive legal regime should impose strict reporting timelines, criminal liability for concealment, and transparent disclosure obligations to ensure accountability and protection of citizens' digital rights.

5) Cross-Border Cybercrime

Cross-border cybercrime involves foreign hackers, multinational criminal organizations, or overseas entities targeting Indian databases, financial systems, or critical

[8] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[9] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

digital infrastructure. Cyberattacks frequently originate outside national boundaries, making investigation and prosecution extremely difficult. Different countries follow different legal standards regarding privacy, data protection, and cybercrime enforcement. Indian agencies often face challenges in obtaining electronic evidence from foreign jurisdictions or identifying anonymous cybercriminals operating through encrypted networks. Existing Indian laws provide limited clarity regarding international jurisdiction and extradition mechanisms in cybercrime cases. Therefore, India requires stronger international cooperation, cybercrime treaties, and cross-border investigative frameworks to effectively combat transnational data breaches and protect national digital security.

The current Indian legal framework inadequately addresses these dimensions because criminal liability provisions remain scattered across multiple statutes without a unified enforcement mechanism. A comprehensive legal framework is therefore essential to ensure effective accountability, stronger cybersecurity standards, and protection of privacy in India's rapidly expanding digital society.

Judicial Approach towards Data Protection and Cyber Accountability

Indian courts have increasingly recognized the importance of privacy and cybersecurity in the digital era.

In *Shreya Singhal v. Union of India*[10], the Supreme Court emphasized the need to balance digital freedom with legal accountability.

In *Anvar P.V. v. P.K. Basheer*, the Court clarified the evidentiary value of electronic records, which has direct implications for cybercrime prosecution and digital investigations.

Judicial decisions have contributed to the development of cyber jurisprudence, yet courts continue to face difficulties concerning:

- Jurisdictional complexities
- Electronic evidence authentication
- Attribution of cyberattacks
- Corporate criminal liability
- Enforcement against multinational entities

Comparative International Approaches

European Union

The General Data Protection Regulation establishes strict obligations concerning data protection, breach notification, and penalties. Organizations may face severe financial sanctions for non-compliance[11].

United States

The United States adopts sector-specific laws such as HIPAA and state-level breach notification laws. Criminal liability may arise under federal cybercrime statutes.

United Kingdom

The UK Data Protection framework imposes substantial responsibilities upon organizations and provides strong regulatory oversight mechanisms.

Lessons for India

India can learn from international best practices by[12]:

- Establishing mandatory breach reporting
- Defining corporate criminal negligence
- Creating independent cybersecurity regulators
- Strengthening victim remedies
- Improving international cyber cooperation

4. Challenges in Imposing Criminal Liability

The rapid growth of digital technologies and online platforms has significantly increased incidents of cybercrime and data breaches in India. Although legal provisions exist under the Information Technology Act, 2000 and other related laws, imposing effective criminal liability for data breaches remains a major challenge. Technological complexity, weak enforcement mechanisms, and lack of public awareness create serious obstacles in ensuring accountability for cyber offenses[13]. The following challenges particularly affect the implementation of criminal liability in data breach cases.

1) Attribution Problems

One of the biggest challenges in cybercrime investigation is identifying the actual perpetrators behind a data breach. Cybercriminals often use sophisticated technologies such as Virtual Private Networks (VPNs), encrypted communication systems, proxy servers, fake identities, and dark web platforms to conceal their identity and location. In many cases, attackers operate through multiple servers located in different countries, making digital tracing extremely difficult. Furthermore, cyberattacks may involve automated malware or bot networks that complicate attribution. Due to these technological barriers, investigative agencies frequently struggle to collect reliable evidence proving who committed the offense. The absence of accurate attribution weakens criminal prosecution and allows many cyber offenders to escape punishment[14].

2) Jurisdictional Issues

Cybercrimes are not restricted by geographical boundaries and frequently involve cross-border operations. A data breach affecting Indian users may originate from servers or individuals located outside India. This creates serious jurisdictional conflicts because different countries follow different cyber laws, privacy regulations, and extradition procedures. Indian investigative agencies often face difficulties in obtaining digital evidence stored on foreign

[10] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[11] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council (2016).
[12] Ministry of Electronics and Information Technology, Government of India, Report on Cyber Security and Data Protection (2024).
[13] Talwant Singh, *Cyber Space and the Law: Issues and Challenges* 210 (Universal Law Publishing, 2020).
[14] Aparna Viswanathan, *Cyber Law: Indian and International Perspectives* 145 (LexisNexis, 2nd ed. 2021).

servers or securing cooperation from international companies. Delays in mutual legal assistance and lack of uniform international cybercrime standards further complicate prosecution. In many situations, offenders exploit jurisdictional gaps between nations to avoid legal action. Therefore, effective criminal liability requires stronger international cooperation and harmonized cybercrime enforcement mechanisms.

3) Lack of Cybersecurity Standards

India currently lacks uniform and mandatory cybersecurity standards applicable across all sectors handling sensitive personal data. Different industries follow different levels of security practices, resulting in inconsistent protection of digital information. Many organizations, especially smaller businesses and local institutions, fail to implement proper encryption systems, firewall protection, employee training, or regular cybersecurity audits. In the absence of standardized security requirements, it becomes difficult to determine whether a corporation acted negligently in protecting data[15]. This legal uncertainty weakens accountability and creates loopholes for organizations to avoid responsibility after data breaches. A comprehensive legal framework should therefore establish clear and sector-specific cybersecurity obligations for all entities processing personal information.

4) Weak Enforcement Infrastructure

Another major challenge is the weak enforcement infrastructure available for investigating and prosecuting cyber offenses. Cybercrime investigation requires specialized technical expertise, digital forensic tools, trained personnel, and modern technological infrastructure. However, many police departments and investigative agencies in India face shortages of skilled cyber experts and forensic laboratories. Delays in investigation, improper handling of electronic evidence, and lack of coordination between agencies further weaken prosecution. Courts may also face difficulties in understanding complex technological evidence. In semi-urban and developing regions, cybercrime cells often lack adequate resources to address sophisticated digital offenses. Strengthening cyber forensic capabilities and institutional training is therefore essential for effective criminal enforcement.

5) Corporate Resistance

Technology companies and large corporations may resist strict criminal liability frameworks due to concerns regarding compliance costs, operational burdens, and reputational risks. Many organizations prefer self-regulation and administrative penalties rather than criminal prosecution for negligence-related data breaches. Corporations may argue that strict liability discourages innovation and increases business expenses. Some companies also hesitate to disclose data breaches because public disclosure may damage consumer trust and market reputation. This resistance often influences policymaking and delays stronger regulatory reforms. However, without effective corporate accountability, organizations may continue to prioritize profit over data protection and cybersecurity responsibilities.

6) Low Public Awareness

Low public awareness regarding digital rights and cybersecurity practices is another significant obstacle in addressing data breaches. Many citizens lack knowledge about privacy rights, online fraud prevention, password security, phishing attacks, and legal remedies available after cyber incidents. Victims often fail to report cybercrimes due to fear, lack of confidence, or ignorance about complaint mechanisms[16]. Poor cyber hygiene practices such as weak passwords, unsafe internet usage, and careless sharing of personal information further increase vulnerability to data breaches. Public awareness campaigns, digital literacy programs, and cybersecurity education are therefore necessary to strengthen individual protection and improve reporting of cyber offenses.

Special Reference to Jodhpur and Emerging Digital Societies

The expansion of digital infrastructure in Jodhpur reflects broader transformations occurring across semi-urban and developing digital societies in India. Educational institutions, healthcare systems, municipal services, and banking networks increasingly rely on digital platforms for governance and service delivery.

However, several challenges persist:

- Limited cybersecurity awareness
- Inadequate digital literacy
- Weak institutional preparedness
- Insufficient cybersecurity audits
- Lack of trained cybercrime personnel

Regional cybercrime cells often face difficulties in investigating sophisticated digital offenses due to technological and manpower limitations. This creates an urgent need for localized digital governance models combined with national cybersecurity standards.

5. Need for a Comprehensive Legal Framework

The increasing number of cyberattacks and data breaches in India highlights the urgent need for a specialized and comprehensive legal framework addressing criminal liability in the digital age. Existing laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 provide partial protection, but they remain fragmented and insufficient for addressing complex cybersecurity challenges. A modern legal framework must ensure privacy protection, digital security, corporate accountability, and effective remedies for victims. The following elements are essential for such a framework[17].

1) Statutory Definition of Data Breach

A comprehensive law should clearly define what constitutes a data breach and distinguish between intentional attacks, negligent disclosures, insider misuse, and accidental leaks. The absence of precise legal definitions creates uncertainty

[15] Justice Yatindra Singh, *Cyber Laws* 98 (Universal Law Publishing, 5th ed. 2022).
[16] Pavan Duggal, *Textbook on Cyber Law* 265 (Universal Law Publishing, 2021).
[17] S.R. Bhansali, "Data Protection and Privacy Challenges in India," 12 Indian Journal of Law and Technology 55 (2022).

regarding liability and enforcement. A statutory definition would help investigative agencies, courts, and organizations understand their legal obligations and responsibilities. Clear categorization of offenses would also improve consistency in prosecution and punishment of cyber offenders.

2) Corporate Criminal Accountability

Organizations that collect and process sensitive personal data must be held accountable for failing to implement adequate cybersecurity measures. Presently, corporate liability is largely limited to monetary penalties and civil compensation. A stronger legal framework should impose criminal consequences for gross negligence, deliberate concealment of breaches, or repeated violations of cybersecurity obligations. Criminal accountability would encourage corporations to prioritize data security and adopt responsible digital governance practices.

3) Mandatory Cybersecurity Compliance

India currently lacks uniform cybersecurity standards applicable across all sectors. A comprehensive legal framework should establish mandatory security protocols relating to encryption, firewall systems, cybersecurity audits, employee training, and risk assessment. Uniform compliance standards are necessary for banks, healthcare institutions, educational organizations, e-commerce platforms, and government agencies handling sensitive information. Such measures would reduce vulnerabilities and strengthen protection against cyberattacks and unauthorized data access.

4) Stronger Data Breach Notification Rules

Organizations should be legally required to promptly disclose data breaches to regulators and affected individuals. Timely disclosure allows victims to take preventive measures such as changing passwords, blocking bank accounts, or monitoring financial transactions. Strict reporting timelines and penalties for concealment should be introduced to ensure transparency and accountability. Effective notification mechanisms would also help regulatory authorities investigate cyber incidents more efficiently and minimize further damage.

5) Victim Compensation Mechanism

Victims of data breaches often suffer financial losses, identity theft, reputational harm, and emotional distress. Therefore, the legal framework should provide accessible and speedy compensation mechanisms for affected individuals. Simplified grievance redressal systems, digital complaint portals, and victim support services should be established. Compensation should reflect the nature and seriousness of the harm caused by the breach. Strong victim-centric remedies would increase public trust in digital systems and legal institutions.

6) Specialized Cybercrime Courts

Cyber offenses involve highly technical evidence and complex digital investigations. Regular courts may face delays due to lack of technological expertise and increasing case burdens. Establishing specialized cybercrime courts or tribunals would improve efficiency in handling digital offenses. Such courts should include trained judicial officers and technical experts capable of understanding electronic evidence, cyber forensics, and digital investigations. Faster adjudication would strengthen cybercrime enforcement and reduce pendency of cases.

7) International Cooperation

Cybercrimes frequently involve foreign hackers, multinational corporations, and servers located outside India. Effective criminal liability therefore requires strong international cooperation. India should strengthen cybercrime treaties, extradition arrangements, and mutual legal assistance agreements with other countries[18]. International collaboration is necessary for obtaining electronic evidence, tracing offenders, and prosecuting cross-border cybercriminals. Harmonized global cybersecurity standards would also improve international enforcement mechanisms and digital security cooperation[19].

8) Capacity Building

Effective implementation of cyber laws requires trained police officers, prosecutors, forensic experts, and judicial officers. Many enforcement agencies currently lack technical expertise and digital investigative resources. Specialized training programs in cyber law, digital evidence collection, and cyber forensics should therefore be introduced. Educational institutions and law universities should also promote cyber law education and research. Capacity building is essential for improving institutional preparedness and effective prosecution of digital offenses.

9) Protection of Digital Privacy

Any comprehensive legal framework must protect the constitutional right to privacy recognized in Justice K.S. Puttaswamy v. Union of India. The framework should ensure lawful, fair, and transparent processing of personal data while preventing arbitrary surveillance and misuse of information. Strong safeguards are necessary to balance national security interests with individual freedoms and digital autonomy. Privacy protection should remain the central objective of all data protection and cybersecurity laws[20].

10) Public Awareness Programs

Public awareness is essential for preventing cybercrime and strengthening digital security. Many citizens remain unaware of phishing attacks, online fraud, password protection, and data privacy rights. Governments, educational institutions, and private organizations should conduct awareness campaigns regarding safe internet practices and cybersecurity measures. Digital literacy programs should be promoted in both urban and rural areas to educate citizens about cyber risks and legal remedies. Increased awareness would reduce vulnerability to cyberattacks and encourage timely reporting of data breaches[21].

[18] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2021).
[19] Nandan Kamath, "Cybersecurity and Corporate Liability in India," 8 National Law School Journal 112 (2023).
[20] Indian Computer Emergency Response Team (CERT-In), *Guidelines on Cyber Security Incident Reporting* (2022).
[21] Reserve Bank of India, *Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices* (2023).

6. Suggestions and Recommendations[22]

1) India should enact a comprehensive cybersecurity legislation integrating privacy, security, and criminal accountability.
2) Criminal liability should extend to corporate executives responsible for serious negligence.
3) The government should establish a National Cybersecurity Authority with investigative powers.
4) Sector-specific cybersecurity standards must be periodically updated.
5) Universities and legal institutions should introduce specialized cyber law education.
6) Digital literacy programs should be promoted at local and regional levels including cities such as Jodhpur.
7) Cyber forensic laboratories should be strengthened across states.
8) Whistleblower protections should be introduced for reporting cybersecurity failures.
9) India should encourage ethical hacking and cybersecurity research.
10) Data protection enforcement mechanisms should remain transparent and independent.

7. Conclusion

The growth of Indian digital societies has generated unprecedented opportunities for economic development, governance efficiency, and technological innovation. Simultaneously, it has exposed individuals and institutions to serious risks arising from cyberattacks and data breaches. The existing Indian legal framework, though evolving, remains fragmented and insufficient in addressing criminal liability for data breaches comprehensively.

While the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 provide partial safeguards, they do not establish a robust criminal accountability mechanism capable of addressing modern cybersecurity threats. The constitutional recognition of privacy as a fundamental right demands stronger legal protection against unauthorized access and misuse of personal data.

India must therefore move toward a comprehensive legal framework that integrates privacy protection, cybersecurity obligations, corporate accountability, victim compensation, and effective criminal enforcement. Such reforms are essential not only for protecting individual rights but also for strengthening public trust in digital governance and technological systems. The challenges faced by emerging digital societies such as Jodhpur further highlight the importance of localized institutional preparedness and national legal reforms.

A balanced and future-oriented legal regime can ensure that India's digital transformation remains secure, accountable, and constitutionally compliant in the years ahead.

[22] Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management Guidelines* (2022).