IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Corporate Liability In Data Breach Cases Under Indian Law

Abstract

In an era dominated by digitalization, corporate liability in data breach cases has become a pressing concern in India's legal and regulatory landscape. Indian corporations are increasingly custodians of vast quantities of sensitive personal data, making them attractive targets for cyberattacks. However, the existing legal framework, comprising primarily the Information Technology Act, 2000 and related rules, has not evolved in tandem with the complexity and scale of contemporary data breaches. This has led to significant ambiguity in assigning corporate accountability. While Section 43A of the IT Act imposes civil liability for failure to protect sensitive personal data, its enforcement remains weak, and it lacks specific criminal provisions for gross negligence or willful data misuse. Furthermore, the absence of a dedicated data protection statute has contributed to inconsistent jurisprudence and inadequate remedies for victims.

The impending Digital Personal Data Protection Act, 2023 promises to fill some of these gaps by introducing clearer obligations, higher penalties, and recognition of fiduciary responsibilities of data fiduciaries. Nonetheless, challenges remain in the form of corporate compliance, regulatory enforcement, and judicial interpretation. Multinational companies operating in India also face dual compliance burdens under foreign data protection laws like the GDPR. Judicial decisions in India have started recognizing privacy as a fundamental right under Article 21, but corporate accountability mechanisms need to be firmly grounded in enforceable legal duties and not just policy declarations. As India moves towards a more robust data governance framework, corporate liability in data breach cases must be restructured to ensure deterrence, victim compensation, and systemic cybersecurity resilience.

Keywords: Corporate liability, data breach, Indian IT law, data protection, digital compliance.

I. Introduction

The data has emerged as a critical asset for corporations, driving everything from targeted marketing and customer service to product development and strategic planning. However, with this growing dependence on digital data comes an increased vulnerability to cyber threats, especially data breaches. These breaches can result in significant harm to individuals, including identity theft, financial loss, and psychological distress, and can severely impact corporate reputation, shareholder value, and legal standing. In India, where digital transactions and data exchanges have exponentially increased due to the expansion of e-governance, fintech services, and e-commerce platforms, the threat of data breaches is no longer theoretical. The growing frequency and severity of such incidents underscore the need to examine the extent to which corporations can and should be held liable under Indian law for data security lapses. The concept of corporate liability in data breach cases involves the imposition of legal responsibility on companies for failing to protect the personal data of individuals they collect, store, and process. In India, this liability primarily arises under the Information Technology Act, 2000 (IT Act), especially Section 43A, which mandates compensation for negligence in implementing reasonable security practices. However, this provision is limited in scope and often criticized for its lack of specificity and weak enforcement mechanisms. Moreover, the absence of a comprehensive data protection statute has led to a fragmented and inconsistent regulatory framework, resulting in uncertainty for corporations and inadequate protections for individuals affected by data breaches.

India's recognition of the right to privacy as a fundamental right under Article 21 of the Constitution, as affirmed by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017), has given new constitutional dimensions to the debate on corporate data responsibility. While the judgment underscored the state's obligation to protect citizens' informational privacy, it also implied a role for private entities—especially large corporations—as data fiduciaries responsible for upholding the trust of data subjects. Despite this evolving constitutional landscape, the legal regime remains ill-equipped to address the complex nature of corporate accountability in cases of cyber negligence or malicious data practices. This lacuna becomes especially concerning given the rising instances of corporate data breaches in sectors such as banking, telecommunications, healthcare, and e-commerce. The proposed Digital Personal Data Protection Act, 2023, seeks to address many of these gaps by introducing clearer duties for data fiduciaries, stringent penalties for violations, and procedural mechanisms for grievance redressal. It emphasizes accountability through consent requirements, purpose limitation, and data minimization principles. However, corporate liability under this new regime will depend heavily on its actual implementation, the strength of regulatory oversight by the Data Protection Board, and the judiciary's interpretation of its provisions. Furthermore, the Act's focus on digital personal data, while necessary, may not be sufficient to tackle emerging concerns in the broader data ecosystem, including data generated through artificial intelligence and the Internet of Things (IoT).

Corporate liability in the Indian context is also complicated by the nature of corporate structures and outsourcing practices. Many companies outsource their data processing tasks to third-party vendors or foreign entities, creating multiple layers of accountability and often blurring the lines of legal responsibility. In such scenarios, questions arise about whether liability should rest with the data controller, the data processor, or both. Indian law has yet to develop comprehensive jurisprudence in this area, and courts have occasionally struggled to establish clear liability, particularly where the breach results from vendor negligence or cross-border data flows. This calls for legal reforms that not only define corporate obligations more precisely but also delineate the standards for due diligence and third-party oversight. Another critical aspect of corporate liability is the intersection of data breaches with consumer protection and contract law. In cases where customers suffer financial or reputational loss due to a corporate data breach, they may seek redress under the Consumer Protection Act, 2019, which recognizes the right to data protection as part of a consumer's right to safety. However, most user agreements between corporations and consumers contain extensive disclaimers and waiver clauses that limit corporate responsibility. This raises significant questions about the fairness and enforceability of such contractual terms in the light of public policy and constitutional protections. The judiciary will have to strike a balance between corporate autonomy and consumer rights to ensure that private entities do not exploit legal loopholes to escape liability. It is also important to analyze India's position in comparison with global best practices, especially with regulations like the European Union's General Data Protection Regulation (GDPR), which imposes strict data protection obligations and holds corporations directly accountable for data breaches. Unlike Indian law, the GDPR imposes both administrative fines and civil liability, ensuring deterrence and victim compensation. Indian regulators and lawmakers can derive valuable insights from such global frameworks to structure a more rigorous and enforceable corporate liability regime. Adopting international standards such as privacy-by-design, mandatory breach notification, and corporate data audits can strengthen corporate accountability and create a safer digital environment for users.

In conclusion, the issue of corporate liability in data breach cases is not just a matter of regulatory compliance but also one of ethical responsibility and public trust. As India moves towards greater digitization and data-driven governance, the legal framework must evolve to ensure that corporations are held accountable for data protection failures. A robust liability regime will not only safeguard individual rights but also incentivize better corporate cybersecurity practices, thereby fostering a digital economy that is both dynamic and secure. The intersection of constitutional rights, statutory mandates, contractual obligations, and international influences makes this area of law complex but undeniably critical for the future of India's digital transformation.

1.1 Role of Regulatory Bodies and Enforcement Challenges

- **Computer Emergency Response Team – India (CERT-In)**

  CERT-In is India's nodal agency for responding to cybersecurity incidents. While it is primarily tasked with issuing advisories and coordinating responses to cyber threats, its role in enforcing corporate accountability in data breaches is limited. It lacks quasi-judicial powers, which restricts its ability to impose penalties or compel compliance. CERT-In's guidelines are often treated as recommendations rather than binding obligations. In major breach incidents, its intervention has been reactive rather than preventive. The absence of a robust monitoring framework under CERT-In reduces its effectiveness in regulating corporate conduct related to data security. Strengthening its mandate with legal backing is essential.

- **Ministry of Electronics and Information Technology (MeitY)**

  MeitY plays a crucial role in formulating policies and laying down rules under the Information Technology Act. It is also responsible for drafting key frameworks like the Digital Personal Data Protection Bill, 2023. However, MeitY's role in enforcement is largely indirect, as it lacks a field-level enforcement apparatus. Its policy-oriented nature often delays real-time interventions in data breach cases. There is also a lack of coordination between MeitY and investigative bodies like CERT-In and law enforcement. Bridging the gap between policy formulation and enforcement is critical to enhancing MeitY's effectiveness.

- **Lack of a Dedicated Data Protection Authority (Pre-2023)**

  The proposed Digital Personal Data Protection Act, 2023, India did not have a dedicated regulatory authority for personal data protection. This institutional vacuum led to fragmented oversight, with different authorities handling different aspects of data regulation. The absence of a central regulator resulted in inconsistent enforcement and a lack of standardized protocols for breach investigation. This also allowed corporations to exploit jurisdictional ambiguities to avoid accountability. A specialized authority, empowered with adjudicatory and penal powers, is essential to ensure corporate compliance.

- **Data Protection Board under the 2023 Bill**

  The proposed Digital Personal Data Protection Act introduces the Data Protection Board of India as a regulatory and adjudicatory body. It is expected to handle complaints, enforce penalties, and ensure compliance with data protection obligations. However, the operational framework of the Board is still unclear, raising concerns about its autonomy, efficiency, and accessibility to individuals. If the Board lacks independence or is overburdened, it may fail to meet its enforcement objectives. Its success will depend on adequate staffing, clear procedures, and enforcement tools. Public trust in the Board's functioning will be vital for its credibility.

- **Weak Penalty and Compensation Mechanisms**

  The major challenges in holding corporations liable for data breaches is the inadequacy of penalty structures. Under Section 43A of the IT Act, compensation is limited to actual damages, and there is no mechanism for punitive or deterrent penalties. Victims often face difficulties in proving harm, especially in cases involving identity theft or data misuse without financial loss. Moreover, corporations are rarely held accountable in public proceedings, which dilutes deterrence. The proposed penalty regime under the 2023 Act needs to incorporate substantial fines that are proportionate to the scale of the breach.

- **Enforcement Delays and Judicial Backlogs**

  India's overburdened judiciary and slow adjudication process have a direct impact on enforcement in cyber law cases. Victims of corporate data breaches rarely pursue litigation due to prolonged timelines and limited awareness of legal rights. Additionally, courts often lack the technical expertise to assess cybersecurity lapses, leading to inconsistent decisions. The absence of cyber-specific benches or tribunals adds to these enforcement challenges. Expedited grievance redressal mechanisms and technical support systems within the judiciary can help streamline corporate accountability proceedings.

- **Non-Mandatory Breach Notification Requirements**

  Unlike the GDPR, Indian law currently does not mandate corporations to notify users or authorities about data breaches, except under CERT-In guidelines which are advisory in nature. As a result, many data breaches go unreported or are disclosed after significant delays. This deprives victims of the opportunity to take timely protective measures and hinders regulatory oversight. Mandatory breach notification provisions in the new data protection law must be strictly enforced. Penalties for concealment or delayed reporting should be clearly codified and applied without exception.

- **Regulatory Fragmentation and Overlap**

  India's regulatory landscape is fragmented, with overlapping responsibilities among agencies like MeitY, RBI (for fintech), TRAI (for telecom), and sector-specific regulators. This leads to confusion over jurisdiction and accountability when a data breach occurs. Corporations exploit this regulatory overlap to avoid clear liability. A harmonized enforcement mechanism that facilitates inter-agency coordination is essential. The proposed Data Protection Board should serve as a centralized authority with overarching jurisdiction over personal data protection across sectors, ensuring consistent enforcement of corporate obligations.

II. Review of Literature

The journey into understanding *corporate liability in data breach cases under Indian law* begins with the foundational legal scholarship of Justice Yatindra Singh, whose book *Cyber Laws* (Universal Law Publishing, 2012) offers one of the earliest and most accessible overviews of India's Information Technology Act, 2000. Singh discusses how the legislation was initially focused more on promoting e-

commerce than addressing data security. He critiques the Act's silence on corporate accountability beyond civil damages and calls for a more rigorous enforcement mechanism to deal with cybercrimes involving corporate negligence. His early warnings about the loopholes in data protection mechanisms proved prophetic as India later faced large-scale corporate data breaches without strong legal remedies.

In 2014, Pavan Duggal, a renowned cyber law expert, contributed extensively through his work *Cyberlaw: The Indian Perspective* (Saakshar Law Publications), where he analyzed the implementation of Section 43A of the IT Act. Duggal pointed out that despite its existence, the provision lacked bite due to vague definitions of "reasonable security practices." He advocated for stronger deterrents and suggested aligning Indian laws with global standards like the GDPR, which was gaining momentum in Europe at the time. Duggal's insights remain vital for understanding how enforcement gaps persist even when legal provisions exist. Moving into a more comparative domain, Graham Greenleaf's *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, 2014) offers an in-depth look at data protection trends across Asia, including India. Greenleaf critically compares Indian law with that of other countries and categorically states that India's data protection regime was among the weakest in Asia, both in enforcement and statutory design. He highlights how India's reliance on rule-based protection under the IT Act contrasts with the rights-based approach seen in stronger legal systems like Japan and South Korea. His work emphasizes the need for a more rights-oriented structure that integrates corporate liability with privacy as a human right.

The conversation shifted significantly after the Supreme Court's landmark ruling in *Justice K.S. Puttaswamy v. Union of India* (2017). Legal scholars such as Dr. Aparna Chandra, in her article *The Right to Privacy in India: The Supreme Court's Verdict and the Way Forward* (Indian Journal of Constitutional Law, 2018), explored how the Court's recognition of privacy as a fundamental right changed the landscape. Chandra discussed how this recognition imposed indirect constitutional obligations on private corporations and increased the urgency for a standalone data protection law. Her work bridges the gap between constitutional jurisprudence and private-sector accountability, highlighting the judiciary's potential in influencing corporate conduct through the doctrine of horizontal application of rights.

The need for reform found further reinforcement in Justice B.N. Srikrishna Committee's *White Paper on Data Protection Framework for India* (2017), which laid the groundwork for the upcoming Digital Personal Data Protection Act, 2023. The committee's report emphasized that corporations acting as "data fiduciaries" have a duty of care toward data principals and recommended high penalties for breaches. It proposed key principles like purpose limitation, data minimization, and accountability, which were inspired by the GDPR. This report has served as a blueprint for India's data protection reforms and introduced a clear legal and ethical narrative around corporate liability.

Meanwhile, Dr. Ramesh Subramaniam, in his book *Information Technology and Legal Framework* (Eastern Book Company, 2019), delved into the failure of Indian regulatory agencies in penalizing corporate defaulters. He documented case studies of data breaches in the Indian banking and telecom sectors and noted that despite substantial consumer harm, regulators failed to hold companies accountable. His work

shows that the problem is not always the absence of law, but the inertia in implementation and absence of judicial activism in cyber law enforcement. Another critical contribution came from Solove and Schwartz, whose global comparative text *Information Privacy Law* (Aspen Publishers, 6th ed., 2020) offers an international lens on how data protection laws affect corporate practices. Though not focused solely on India, the book's analysis of GDPR's strict liability model and its contrast with the U.S.'s sectoral approach gives Indian scholars a framework to critique the limited reach of Indian laws. Their emphasis on legal certainty and enforcement architecture adds to the understanding of what Indian law lacks in the corporate liability context.

In more recent literature, Kumar and Wadhwa's journal article *Corporate Accountability in the Age of Data Breaches: Legal Challenges in India* (NUJS Law Review, 2021) presents an up-to-date analysis of how Indian companies respond to data breaches. They argue that most corporations use contractual loopholes and vague privacy policies to escape liability. The authors propose reforms including mandatory breach disclosure, independent audits, and the recognition of a right to data compensation. This article stands out for combining empirical case studies with legal critique and offers practical recommendations. Apart from this, Mehta and Rao, in their 2023 book *Digital Governance and Privacy in India* (Bloomsbury India), bring the discussion into the present moment by evaluating the Digital Personal Data Protection Bill, 2023. They assess its strengths—such as penalty structures and grievance redressal mechanisms—and weaknesses, like the lack of clarity on the role of the Data Protection Board. They caution that unless enforcement is proactive and victim-centric, the law may turn into yet another compliance checklist for corporations. Their work stresses the importance of regulatory will in translating statutory language into actual corporate accountability.

Together, these contributions create a rich tapestry of insights, critiques, and proposals that help chart the path forward. They collectively show that while Indian legal scholarship has recognized the need for stronger corporate liability in data breach cases, the real challenge lies in enforcement, judicial consistency, and public awareness. The literature firmly supports the argument that corporate accountability must move beyond token compliance toward a regime of legal responsibility grounded in both constitutional values and global best practices.

III. Research Methodology

This study adopts a doctrinal legal research methodology, focusing on the analysis of primary and secondary legal sources to explore the concept of corporate liability in data breach cases under Indian law. The research is qualitative in nature and involves a comprehensive review of statutory provisions, judicial precedents, government reports, and policy frameworks. Key legislations such as the Information Technology Act, 2000—particularly Sections 43A and 72A—have been examined to assess how they impose liability on corporations for data breaches. Constitutional developments, especially the Supreme Court's ruling in *Justice K.S. Puttaswamy v. Union of India* (2017), are analyzed to understand how the right to privacy has broadened the scope of legal accountability for private data processors. The study also

engages with the draft provisions of the upcoming Digital Personal Data Protection Act, 2023 to evaluate the direction of legal reform in India's data protection regime.

The research employs a comparative approach by examining international standards, particularly the European Union's General Data Protection Regulation (GDPR), to highlight the structural deficiencies in Indian law. Secondary sources such as academic journals, expert committee reports, and case studies involving real data breach incidents in Indian corporations are critically reviewed to identify enforcement gaps, judicial inconsistencies, and areas of weak compliance. While the study does not include empirical data or field surveys, selected case law analysis and regulatory responses have been used to illustrate how legal provisions operate in practice. This methodology supports a critical and normative evaluation of the existing legal framework and offers recommendations for strengthening corporate accountability in the context of data protection.

IV. Result and Discussion

The findings of the present study on corporate liability in data breach cases under Indian law reveal a complex and evolving legal landscape marked by significant gaps in regulation, enforcement, and jurisprudence. A critical analysis of existing statutes, including the Information Technology Act, 2000, shows that although some provisions attempt to address corporate responsibility—most notably Section 43A and Section 72A—the enforcement of these provisions remains minimal and largely reactive rather than preventive. The statutory language lacks precision in defining "reasonable security practices," leading to wide discretion and varied interpretations by corporations and regulators. As a result, companies often adopt a compliance-minimum attitude, wherein the primary goal is to avoid legal exposure rather than protect user data substantively. Moreover, very few high-profile data breach cases in India have resulted in meaningful penalties or judicially imposed corporate liability, highlighting systemic deficiencies in adjudication and regulatory action. The empirical data and case studies point toward a lack of deterrence and accountability. Many corporations delay notifying users or authorities about data breaches, and in some cases, breaches are never disclosed publicly. This lack of transparency not only undermines user trust but also prevents regulatory agencies from taking timely action. A comparative analysis with international frameworks, especially the European Union's General Data Protection Regulation (GDPR), underscores India's lag in critical areas such as mandatory breach notifications, data minimization principles, and corporate data audits. Under the GDPR, corporations are not only held strictly accountable but are also obligated to maintain transparency and fairness, something Indian law fails to mandate effectively.

Judicial responses to corporate data breaches in India have also been inconsistent and limited. Although the *Puttaswamy* judgment elevated informational privacy to a constitutionally protected right, Indian courts have yet to develop a coherent doctrine on corporate accountability in data protection matters. Where petitions have been filed, outcomes often depend on the specific facts of each case, and there is no uniform standard guiding corporate obligations. Additionally, courts tend to rely on contract law and tort principles,

such as negligence or breach of duty, which may not always align with the technical complexities of data security. The absence of specialized data protection tribunals or technical benches in the judiciary has further contributed to a lack of jurisprudential clarity and speed in resolving such disputes. The business practices of Indian corporations also reflect a general underestimation of the seriousness of data security. Many firms, especially small and medium enterprises (SMEs), either lack robust data protection infrastructure or outsource data management to third-party vendors without ensuring adequate oversight. Even in larger organizations, cybersecurity budgets and strategies are often reactive, implemented after a breach rather than as a preventative measure. This laxity in attitude can be traced to a regulatory ecosystem that has not consistently penalized failures or incentivized best practices. Notably, user agreements and privacy policies often contain broad disclaimers that shift the burden of risk to the user, further diluting corporate accountability. In many cases, users are not even aware of the rights they possess or the recourses available to them.

The proposed Digital Personal Data Protection Act, 2023, represents a landmark development that could significantly reshape the legal accountability of corporations. It introduces the concept of data fiduciaries, places consent at the center of data processing, and prescribes penalties for data breaches. However, it remains to be seen how rigorously these provisions will be implemented, especially given India's past record of regulatory enforcement. The success of this framework will depend on the establishment of an empowered Data Protection Board, clearly defined compliance mechanisms, and timely judicial intervention when violations occur. Importantly, the Act must avoid over-reliance on bureaucratic processes and ensure accessible grievance redressal mechanisms for affected individuals. In addition, the cross-border nature of data processing and cloud storage presents a jurisdictional challenge. Indian companies operating internationally must comply with foreign laws like the GDPR, while foreign companies operating in India often exploit jurisdictional ambiguities to evade liability. This duality creates uncertainty and legal conflict, often leaving victims in a grey zone without adequate remedies. A harmonized legal framework that addresses transnational data transfers and clearly identifies corporate obligations, irrespective of geographical boundaries, is urgently required. Moreover, India must actively engage in international dialogues on data governance to align its domestic law with global best practices while safeguarding its sovereignty and data economy.

In summary, the results demonstrate that corporate liability in data breach cases in India is inadequately structured, inconsistently enforced, and insufficiently supported by judicial and regulatory mechanisms. The lack of a coherent legal and institutional framework has allowed corporations to operate with minimal accountability, often at the expense of consumer rights and digital trust. The proposed legislative reforms offer a promising start but must be complemented by judicial clarity, regulatory competence, and public awareness. Strengthening corporate liability is not merely a legal imperative—it is essential for building a resilient, privacy-respecting, and trustworthy digital economy in India.

V. Conclusion

The issue of corporate liability in data breach cases under Indian law is at a critical juncture. As data becomes the backbone of modern commerce and governance, the risks associated with its mishandling have become increasingly consequential. Indian corporations, entrusted with vast troves of sensitive personal and financial information, are facing rising scrutiny for lapses in data security. While the Information Technology Act, 2000 has served as a foundational legal instrument, its outdated provisions and limited enforcement capabilities have proven inadequate to address the evolving landscape of cyber threats. The absence of a comprehensive and enforceable data protection framework has resulted in fragmented accountability and inconsistent protections for data subjects. The recognition of the right to privacy as a fundamental right by the Supreme Court of India in the *Puttaswamy* judgment has expanded the scope of corporate responsibility, implicitly placing the onus on private entities to act as data fiduciaries. However, meaningful enforcement of such constitutional ideals requires robust statutory mechanisms. The upcoming Digital Personal Data Protection Act, 2023 represents a significant step forward, offering clearer guidelines, stronger penalties, and a regulatory structure to monitor corporate compliance. Yet, the true effectiveness of this legislation will depend on its implementation, judicial interpretation, and the proactive role of regulatory bodies.

Going forward, India must prioritize legal reforms that impose well-defined obligations on corporations, ensure swift redressal for victims, and establish deterrent penalties for data breaches. In a global digital economy, harmonizing domestic law with international data protection standards is equally important. Ultimately, holding corporations accountable for data breaches is essential not only to protect individual rights but also to build a trustworthy and secure digital ecosystem.

References

- Chandra, A. (2018). *The Right to Privacy in India: The Supreme Court's Verdict and the Way Forward*. *Indian Journal of Constitutional Law*, 8(1), 123–147.
- Duggal, P. (2014). *Cyberlaw: The Indian Perspective* (5th ed.). New Delhi: Saakshar Law Publications.
- Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press.
- Justice Srikrishna Committee. (2017). *White Paper on Data Protection Framework for India*. Ministry of Electronics and Information Technology. Retrieved from https://www.meity.gov.in/
- Kumar, A., & Wadhwa, R. (2021). Corporate Accountability in the Age of Data Breaches: Legal Challenges in India. *NUJS Law Review*, 14(2), 89–116.
- Mehta, A., & Rao, V. (2023). *Digital Governance and Privacy in India*. New Delhi: Bloomsbury India.
- Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Bill, 2023*. Government of India. Retrieved from https://www.meity.gov.in/
- Singh, Y. (2012). *Cyber Laws*. Universal Law Publishing.

- Solove, D. J., & Schwartz, P. M. (2020). *Information Privacy Law* (6th ed.). Aspen Publishers.
- Subramaniam, R. (2019). *Information Technology and Legal Framework*. Lucknow: Eastern Book Company.
- Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Tiwari, S. (2020). Data Breaches and Corporate Liability: A Regulatory Analysis. *Indian Journal of Law and Technology*, 16(1), 56–75.
- CERT-In. (2022). *Guidelines for Cybersecurity Incident Reporting*. Computer Emergency Response Team – India. Retrieved from https://www.cert-in.org.in/
- Ramanathan, U. (2018). Privacy and the Private Sector in India: Weak Protection, Little Accountability. *Economic and Political Weekly*, 53(47), 10–14.
- Bhatia, G. (2019). *The Transformative Constitution: A Radical Biography in Nine Acts*. HarperCollins India.