International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

From Section 43A of IT Act to DPDP Act 2023: A Comparative Study of Corporate Liability Vs. State Immunity

Written by- **Manisha and Prince Saini**
Under Special Guidance Of Assistant **Professor Swarnim Chaudhary**

https://doi.org/10.55041/ijsmt.v2i4.420

Cite this Article: Manisha, & Saini, P. (2026). From Section 43A of IT Act to DPDP Act 2023: A Comparative Study of Corporate Liability Vs. State Immunity. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.420

License: This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

Abstract

In the current digital era, data protection has emerged as an indispensable aspect of both individual privacy and national security. This research paper presents a comparative analysis of the evolutionary trajectory of India's legal framework ranging from the erstwhile Section 43A of the Information Technology (IT) Act, 2000, to the new Digital Personal Data Protection (DPDP) Act, 2023. The primary objective of this study is to examine the shifting dynamics between 'Corporate Liability' and 'State Immunity.'

The study indicates that while Section 43A imposed limited civil liability on 'Body Corporates,' the DPDP Act, 2023, has tightened corporate accountability by imposing hefty penalties and statutory duties through the concept of a 'Data Fiduciary.' However, a significant 'research gap' that emerges is the scope of 'State Immunity'. This research highlights how the broad exemptions granted to government agencies under the new law in the name of 'national security' and 'public order' create an 'accountability gap' that stands in contrast to the strict regulations imposed on private corporations. Furthermore, this paper analyzes the shift from the 'compensation-based model' of the IT Act to the 'penalty-based model' of the DPDP Act i.e. a transition that prioritizes the State exchequer over aggrieved citizens. Ultimately, this research paper argues that a balanced data protection framework necessitates ensuring equal accountability for both the State and corporations, thereby safeguarding against the infringement of the 'Right to Privacy' within the context of India's digital inclusion.

Keywords: DPDP Act 2023, Section 43A of the IT Act, Corporate Liability, State Immunity, Data Privacy, Accountability Gap.

Introduction

In the current digital economy, data is viewed not merely as information, but as a valuable economic resource and a source of governance power. In India, the legal journey of data protection began with Section 43A of the Information Technology (IT) Act, 2000, which was introduced through the 2008 amendment.[1] Section 43A introduced, for the first time, the principle of 'Corporate Liability,' holding a 'Body Corporate' liable to pay compensation in the event of negligence in protecting sensitive personal data.[2] However, as the DSCI report and experts suggest, this framework of the IT Act was limited solely to commercial entities, thereby excluding the vast data processing activities of the government machinery from the ambit of

[1] Information Technology Act, 2000, Section 43A, No. 21, Acts of Parliament, 2000 (India).
[2] Yogesh Prasad Kolekar, Protection of Data Under Information Technology Law in India, SSRN (2015).

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

accountability.[3] The landmark judgment in Justice Puttaswamy v. Union of India (2017) declared privacy a fundamental right, thereby reshaping the trajectory of digital jurisprudence.[4] This constitutional mandate led to the enactment of the 'Digital Personal Data Protection (DPDP) Act, 2023.' This Act marks a significant departure from the previous framework, introducing the concept of a 'Data Fiduciary' and stipulating hefty penalties of up to ₹250 crore for data breaches.[5]

According to research, this law imposes strict 'fiduciary' i.e. trust-based obligations upon corporations.[6] However, the most controversial and significant aspect of this new law is 'State Immunity.' While, on the one hand, the regulations for private corporations have been made extremely stringent, on the other, Section 7 of the Act grants the government special exemptions for data processing on broad grounds such as 'national security,' 'relations with foreign states,' and 'public order.[7] Research also points to how data infrastructure is frequently utilized to expand executive powers.[8] Consequently, this research paper undertakes an in-depth analysis of whether the DPDP Act truly provides a balanced protective framework, or if it has merely become a vehicle for granting unbridled immunity to state powers while ostensibly enhancing corporate accountability.[9]

Research Questions

1. What significant changes have occurred in the legislative framework of corporate liability, ranging from Section 43A of the Information Technology Act to the DPDP Act, 2023?

2. Do the broad exemptions granted to the State under the DPDP Act, 2023, create an imbalance between 'corporate accountability' and 'State immunity'?

3. How does the shift from a compensation-based model (Section 43A) to a penalty-based model (DPDP Act) impact the accessibility of justice for victims of data breaches ?

Literature Review

The present research paper analyzes the scholarly works and legal documents that have discussed the evolving landscape of data protection in India. The foundation of data protection in India was laid with Section 43A of the Information Technology (IT) Act, regarding which

[3] Data Security Council of India, Reasonable Security Practices – IT (Amendment) Act, 2008: Study Report 12 (2010).
[4] (2017) 10 S.C.C. 1 (India).
[5] Digital Personal Data Protection Act, 2023, Section 33, No. 22, Acts of Parliament, 2023 (India).
[6] Deepanshu & Dr. Ashok Kumar, Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023, 1 Vistas Int'l J. Multidisciplinary Stud. 4, 10 (2026).
[7] Digital Personal Data Protection Act, 2023, Section 7, No. 22, Acts of Parliament, 2023 (India).
[8] Ramya Chandrasekhar, Datafication, Power, and Publics in India's National Digital Health Ecosystem, 20 Socio-Legal Rev. 1, 15 (2024).[9] Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 142 (2024).

Yogesh Prasad Kolekar (2015) argues that it, for the first time, imposed the principle of civil liability upon 'body corporates' for negligence in safeguarding sensitive data.[10] However, the DSCI (2010) report underscores that the scope of the IT Act was primarily limited to business entities, leaving government data processing within a legal vacuum.[11] Over time, digital transformation transformed data into an economic resource, a point highlighted by Altamash Farahat (2023) in his analysis, wherein he explains how the need for comprehensive legislation became imperative following the Puttaswamy judgment.[12] In this context, research by Deepanshu and Dr. Ashok Kumar (2026) clarifies that the DPDP Act, 2023, has further tightened corporate accountability by introducing the concept of a 'Data Fiduciary,' wherein provisions for hefty penalties now exist.[13] Conversely, Amresh Patel and Dr. Radha Ranjan (2024) draw attention to the extensive exemptions granted to the State, which create a significant disparity in accountability between corporations and the State.[14] Ultimately, Ramya Chandrasekhar's (2024) work frames this imbalance through the lens of 'datafication and power' i.e. a context in which the powers of the state are continuously expanding, while the remedies available for

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

individual rights are becoming increasingly limited.[15] Thus, while existing literature demonstrates that corporate oversight has increased, there remains a dearth of research regarding the conflict between the 'protective immunity' granted to the state and the privacy rights of citizens, a gap that this paper addresses.

The Evolution of Corporate Accountability

The legal journey of data protection in India began with the Information Technology (IT) Act, 2000. Initially, the Act remained silent on the subject of data privacy; however, the 2008 amendment introduced Section 43A, which established the first direct liability for corporate entities.[16]

1.1 Analysis of Section 43A of the Information Technology Act: According to the Bare Act, the text of Section 43A reads as follows: Compensation for failure to protect data.–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of

---

[10] Yogesh Prasad Kolekar, Protection of Data Under Information Technology Law in India, SSRN (2015).
[11] Data Security Council of India, Reasonable Security Practices – IT (Amendment) Act, 2008: Study Report 14 (2010).
[12] Altamash Farahat, Digital Personal Data Protection Act, 2023: A Constitutional and Comparative Analysis, 8 Indian J.L. & Legal Res. 3326 (2023).
[13] Deepanshu & Dr. Ashok Kumar, Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023, 1 Vistas Int'l J. Multidisciplinary Stud. 4, 18 (2026).

[14] Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 155 (2024).
[15] Ramya Chandrasekhar, Datafication, Power, and Publics in India's National Digital Health Ecosystem, 20 Socio-Legal Rev. 1, 25 (2024).

[16] Information Technology (Amendment) Act, 2008, Section 43A, No. 10, Acts of Parliament, 2009 (India).

compensation to the person so affected.[17] Interpreting this section, Yogesh Prasad Kolekar argued that this provision was limited solely to 'compensation'.[18] According to the DSCI (2010) report, the interpretation of 'Reasonable Security Practices' was ambiguous, making it difficult to enforce in the courts.[19]

1.2 The Emergence of 'Data Fiduciary' under the DPDP Act, 2023: The Digital Personal Data Protection (DPDP) Act, 2023, has introduced the broader term 'Data Fiduciary' to replace 'Body Corporate'.According to Section 2(i) of the Bare Act: "Data Fiduciary means any person who, alone or jointly with other persons, determines the purpose and means of processing personal data."[20] According to Deepanshu and Dr. Ashok Kumar, this definition clarifies that the responsibility now extends not merely to the holding of data, but also to the 'purpose' of processing it.[21] Section 8 of the Act imposes a mandatory duty upon the Data Fiduciary to implement reasonable security safeguards for the protection of data. The most significant distinction lies in the Schedule to the Act, which, under Section 33, prescribes the following penalties for data breaches: "Failure to take reasonable security safeguards to prevent a personal data breach: A fine of up to ₹250 crore."[22] This clarifies that the law has now shifted its focus from merely compensating the victim (Section 43A) to imposing substantial penalties on the Data Fiduciary (DPDP Act).

State Immunity

The primary focus of this research paper is the imbalance created by the Digital Personal Data Protection (DPDP) Act, 2023, between the State (Government) and private corporations. While, on one hand, heavy penalties and 'fiduciary' responsibilities have been imposed upon corporate entities, the State, on the other hand, has been granted broad and vague exemptions— a situation that calls into question the 'principle of equality.'

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Analysis of the State's Broad Exemptions and Section 17:

Section 17 of the DPDP Act serves as the primary legal basis for the immunity granted to the State. According to the Bare Act, Section 17(2) states: The provisions of this Act shall not apply in respect of the processing of personal data—(a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and

(b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.[23] According to Altamash Farahat, the scope of terms such as 'Public Order' is so broad that the government can shield any of its data

[17] Information Technology Act, 2000, Section 43A.
[18] Yogesh Prasad Kolekar, Protection of Data Under Information Technology Law in India, SSRN, 1, 4 (2015)
[19] Data Security Council of India, Reasonable Security Practices – IT (Amendment) Act, 2008: Study Report 12 (2010).
[20] Digital Personal Data Protection Act, 2023, § 2(i), No. 22, Acts of Parliament, 2023 (India).
[21] Deepanshu & Dr. Ashok Kumar, Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023, 1 Vistas Int'l J. Multidisciplinary Stud. 4, 12 (2026).
[22] Digital Personal Data Protection Act, 2023, Schedule, No. 22, Acts of Parliament, 2023 (India).
[23] Digital Personal Data Protection Act, 2023, Section 17(2), No. 22, Acts of Parliament, 2023 (India).

processing activities under its ambit.[24] This situation poses a significant challenge to the 'Right to Privacy' established by the Puttaswamy judgment (2017), as it empowers the State to utilize citizens' data without any rigorous oversight.The Accountability Gap and Executive Powers:- According to Ramya Chandrasekhar's research paper, 'Datafication, Power, and Publics,' data is now being utilized by the State to expand its executive powers.[25] For instance, in projects such as the National Digital Health Ecosystem, government agencies collect vast amounts of sensitive data. Since they are granted exemptions under Section 17 in the name of 'good faith' and 'national security,' a citizen's legal remedies against the State become severely limited in the event of a data leak.[26] Amresh Patel and Dr. Radha Ranjan argue that this Act establishes a 'double standard.'[27] While a private 'Data Fiduciary' may face a penalty of up to ₹250 crore under Section 33 (Schedule) for a data security breach, there is a distinct absence of any such punitive liability for government agencies.[28] This imbalance suggests that the law is tilted more towards preserving the 'immunity' of the State than towards safeguarding the citizen.

The Transition from Section 43A to the DPDP Act

This research paper highlights that India's data protection regime has shifted from a 'compensation-centric' framework to a 'penalty-centric' framework. This shift is not merely a matter of terminology, but rather concerns the underlying philosophy of justice. The Conceptual Shift from 'Body Corporate' to 'Data Fiduciary': Under Section 43A of the IT Act, liability was confined to a 'Body Corporate'.[29] According to Yogesh Prasad Kolekar, this was a mere commercial obligation.[30] However, the DPDP Act, 2023, by employing the term 'Data Fiduciary,' has elevated this to the level of a 'trust.' Under Section 8, a corporation's responsibility is no longer limited to merely safeguarding data, but extends to upholding the trust that a citizen reposed in it while providing their data.[31] The End of Compensation and the Rise of Penalties: The most significant and contentious change has occurred regarding the 'Fruits of Justice.' The primary objective of Section 43A was to provide financial relief to the victim. The wording of the Bare Act's "liable to pay compensation to the person affected by the damage" ensured that the money reached the victim.[32] In contrast, under Section 33 (Schedule) and Section 25 of the DPDP Act, a penalty of up to ₹250 crore may be imposed in the event of a violation; however, instead of being received by the aggrieved party, this amount will be deposited into the 'Consolidated Fund of India.'[33] According to Deepanshu and Dr. Ashok Kumar, this 'shift' indicates that the law is now focusing more on strengthening the

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

[24] Altamash Farahat, Digital Personal Data Protection Act, 2023: A Constitutional and Comparative Analysis, 8 Indian J.L. & Legal Res. 3326, 3332 (2023).
[25] Ramya Chandrasekhar, Datafication, Power, and Publics in India's National Digital Health Ecosystem, 20 Socio-Legal Rev. 1, 15 (2024).
[26] Id. at 28.
[27] Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 155 (2024).
[28] Digital Personal Data Protection Act, 2023, Schedule, No. 22, Acts of Parliament, 2023 (India).
[29] Information Technology Act, 2000, Section 43A.
[30] Yogesh Prasad Kolekar, Protection of Data Under Information Technology Law in India, SSRN, 1, 8 (2015).
[31] Digital Personal Data Protection Act, 2023, § 8, No. 22, Acts of Parliament, 2023 (India)
[32] Information Technology Act, 2000, Section 43A.
[33] Digital Personal Data Protection Act, 2023, Section 25, No. 22, Acts of Parliament, 2023 (India).

State's regulatory control rather than on compensating citizens for their personal losses.[34] Deterrence vs. Remedial Approach: While the IT Act was 'remedial' (providing a remedy after harm has occurred), the DPDP Act is 'deterrent' in nature. The objective of imposing heavy penalties is to instill fear in companies, thereby ensuring that they prevent data breaches from occurring in the first place. However, Amaresh Patel and Dr. Radha Ranjan argue that the elimination of compensation could limit the process of seeking justice for citizens to an 'elite' few, as the average citizen would be reluctant to engage in a protracted legal battle without the prospect of any personal benefit.[35]

Section 17 and State Immunity - A Critical Analysis

This research paper highlights that the exemptions granted to the State under the Digital Personal Data Protection (DPDP) Act, 2023, are not merely exceptions; rather, they establish a legal framework wherein the government cannot be held accountable for citizens' rights.

1. Extension of Exemptions under Section 17: Section 17(2) of the Act empowers the Central Government to exempt any of its agencies from all or any of the provisions of the Act. As per the Act, such exemption may be granted on the following grounds: "...in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence."[36] According to Altamash Farahat, terms such as 'Public Order' are so broad that they effectively grant the State a 'blank cheque.'[37] This violates the 'three-fold test' (Legality, Necessity, and Proportionality) laid down by the Supreme Court in the Puttaswamy (2017) case, as there exists no independent judicial or legislative oversight over the State's powers.

2. Accountability Gap: According to Ramya Chandrasekhar, when the State places itself outside the ambit of the law, it creates a 'power imbalance' between citizens and the government.[38] While private entities face severe penalties in the event of data theft, citizens lack effective legal recourse in situations involving the misuse or leakage of data by government agencies. Amresh Patel and Dr. Radha Ranjan argue that this 'protective immunity' granted to the State undermines the very core objective of data protection.[39] This research paper clarifies that, for a balanced framework, it is essential that the exemptions granted in the name of 'national security' be limited and accountable, rather than absolute and unchecked.

[34] Deepanshu & Dr. Ashok Kumar, Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023, 1 Vistas Int'l J. Multidisciplinary Stud. 4, 25 (2026)
[35] Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 142 (2024).
[36] Digital Personal Data Protection Act, 2023, Section 17(2), No. 22, Acts of Parliament, 2023 (India).
[37] Altamash Farahat, Digital Personal Data Protection Act, 2023: A Constitutional and Comparative Analysis, 8 Indian J.L. & Legal Res. 3326, 3332 (2023).
[38] Ramya Chandrasekhar, Datafication, Power, and Publics in India's National Digital Health Ecosystem, 20 Socio-Legal

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Rev. 1, 28 (2024).

39 Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 155 (2024).

Accessibility of Justice and Impact on Victims

This research paper highlights that the transition from the IT Act, 2000, to the DPDP Act, 2023, is not merely technical; rather, it fundamentally alters the very concept of justice. Does this new framework render justice more accessible to aggrieved citizens, or does it effectively exclude them from the legal process?

1. The Disappearance of Compensation and Civil Rights: The central tenet of Section 43A of the IT Act was 'compensation.' According to the language of the Bare Act, if a company was negligent in ensuring data security, it was "liable to pay compensation by way of damages to the affected person."[40] Yogesh Prasad Kolekar argues that this provision placed the victim at the center.[41] If your data was leaked, the court or the Adjudicating Officer would order the company to pay money directly to you (the victim). In contrast, under the DPDP Act, 2023, there is no provision for compensation.Section 33 (Schedule) of the Act stipulates heavy fines; however, Section 25 of the Act clarifies that all such proceeds shall accrue to the 'Consolidated Fund of India.'[42] This implies that an ordinary citizen whose personal data has been leaked stands to gain nothing financially from this entire legal battle. According to Deepanshu and Dr. Ashok Kumar, this model is 'State-centric' rather than 'Victim-centric'—a framework in which the State wields significant power as a regulator, while the citizen is reduced to the role of a helpless spectator.[43] 'State Immunity' and the Struggle for Access to Justice: Access to justice becomes even more arduous when a data breach is perpetrated by the government. As the State enjoys broad immunity under Section 17, filing a complaint against the government is akin to 'running into a mountain.'[44] According to Ramya Chandrasekhar (2024), the government possesses the protective shield of 'national security.'[45] If a government application leaks data, a citizen would find themselves entangled merely in the task of proving whether or not such data processing falls within the scope of an 'exemption.'

2. Judicial Burden and Grievance Redressal Mechanism: The new law establishes a 'Data Protection Board' (DPB); however, in the absence of compensation, it will be difficult for a common person to access the Board. Amresh Patel and Dr. Radha Ranjan argue that unless there is a personal benefit (compensation), citizens will not be incentivized to report data breaches.[46] Furthermore, the Act also limits the jurisdiction of civil courts, thereby further reducing the avenues for seeking justice.4. Conclusion-based Analysis: This analysis clarifies that, throughout the journey from Section 43A to the DPDP Act, 'Corporate Accountability' has indeed increased (driven by the fear of fines amounting to ₹250 crore), yet 'Access to Justice' has diminished. The aggrieved individual has been reduced to a mere 'informant' within the justice delivery process, rather than being recognized as the person entitled to receive

[40] Information Technology Act, 2000, Section 43A, No. 21, Acts of Parliament, 2000 (India).
[41] Yogesh Prasad Kolekar, Protection of Data Under Information Technology Law in India, SSRN, 1, 4 (2015).
[42] Digital Personal Data Protection Act, 2023, Section 25, No. 22, Acts of Parliament, 2023 (India).
[43] Deepanshu & Dr. Ashok Kumar, Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023, 1 Vistas Int'l J. Multidisciplinary Stud. 4, 25 (2026).
[44] Digital Personal Data Protection Act, 2023, Section 17(2), No. 22, Acts of Parliament, 2023 (India).
[45] Ramya Chandrasekhar, Datafication, Power, and Publics in India's National Digital Health Ecosystem, 20 Socio-Legal Rev. 1, 28 (2024).
46 Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 142 (2024).

compensation for the harm suffered. This 'Accountability Gap' and 'Compensation Gap,' taken together, effectively limit the 'Right to Privacy' of Indian citizens to a mere right on paper.

Suggestions

The present research paper highlights that there is ample scope for improvement in the DPDP Act, 2023, in order to strike a balance between State and corporate accountability. Based on this research, the following suggestions are proposed: -

1. Judicial Oversight of State Exemptions: The exemptions granted to the government under Section 17(2) of the Act

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

should not be left 'unfettered.' It is suggested that obtaining prior permission from an independent judicial authority or a 'Data Protection Board' be made mandatory before granting exemptions to state agencies. According to Altamash Farahat, exemptions granted without any independent audit give rise to 'unbridled powers,' which can be curbed through judicial review.[47]

2. Reintroduction of Compensation: The Act should transition from a 'penalty-based' approach to a 'Hybrid Model' (Penalty + Compensation). As stipulated under Section 43A of the IT Act, victims of data breaches should receive direct compensation for their financial or mental distress. Deepanshu and Dr. Ashok Kumar argues that unless victims receive some form of financial relief, the objective of safeguarding civil rights will remain unfulfilled.[48]

3. A Clear Definition of 'Public Order': Broad terms such as 'public order' and 'national security' must be clearly defined within the law. This would reduce the potential for misuse of these terms by government agencies. According to Ramya Chandrasekhar, vague terminology grants the State excessive power over citizen data.[49]

4. Independent Data Protection Board (Independent DPB): The Central Government's interference in the appointment of the Data Protection Board should be minimized. It should be constituted as an autonomous body so that it can impose penalties without any pressure even on the negligence of the government's own agencies.

Conclusion

[47] Altamash Farahat, Digital Personal Data Protection Act, 2023: A Constitutional and Comparative Analysis, 8 Indian J.L. & Legal Res. 3326, 3338 (2023).
[48] Deepanshu & Dr. Ashok Kumar, Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023, 1 Vistas Int'l J. Multidisciplinary Stud. 4, 30 (2026).
[49] Ramya Chandrasekhar, Datafication, Power, and Publics in India's National Digital Health Ecosystem, 20 Socio-Legal Rev. 1, 35 (2024).

The objective of this research paper was to analyze the revolutionary changes that have taken place within India's data protection framework. The journey from the 'limited corporate liability' under Section 43A (IT Act) to the 'strict Data Fiduciary' model of the DPDP Act, 2023, demonstrates that India now recognizes data as a critical economic resource. However, this evolution has come at the cost of a significant 'Accountability Gap'. This research clarifies that while the Act imposes stringent penalties (fines of up to ₹250 crore) on the private sector, it has, through Section 17, provided a 'protective shield' to the State. The argument was advanced by Amresh Patel and Dr. Radha Ranjan appears valid that this law challenges the 'Principle of Equality' (Article 14), wherein a private entity is penalized for a specific type of data breach, while a government entity receives an exemption in the name of 'national security'.[50] The 'non- compensatory' nature of the Act renders the pursuit of justice difficult for victims. While Section 43A of the IT Act placed the citizen at the center, the DPDP Act prioritizes the regulatory control of the State. The 'Right to Privacy' recognized as a fundamental right in the Puttaswamy (2017) case cannot be safeguarded unless both the State and corporations are held equally accountable.Ultimately, this research paper argues that a balanced data protection framework is one that upholds 'Digital Inclusion' alongside 'constitutional safeguards.' India requires a law wherein 'national security' does not entail infringing upon citizens' privacy, but rather serves to further secure it. Only then will we be able to establish a true digital democracy, where data protection is not a means of 'power,' but a guarantee of 'rights'.

[50] Amaresh Patel & Dr. Radha Ranjan, Data Protection and Privacy Laws 160 (2024).

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.