INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 14 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 14 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-14-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CORPORATE LIABILITY FOR BIOMETRIC DATA MISUSE: RECONCEPTUALISING DIRECTOR-SPECIFIC DUTIES IN INDIAN COMPANY LAW

AUTHOR - SARIGA S KUMAR, VELURATHNAKARAN K S, GAYATHRI S R

PG SCHOLARS OF CENTRAL UNIVERSITY OF TAMIL NADU, THIRUVARUR

BEST CITATION - SARIGA S KUMAR, VELURATHNAKARAN K S, GAYATHRI S R, CORPORATE LIABILITY FOR BIOMETRIC DATA MISUSE: RECONCEPTUALISING DIRECTOR-SPECIFIC DUTIES IN INDIAN COMPANY LAW, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (14) OF 2025, PG. 451-457, APIS – 3920 – 0001 & ISSN - 2583-2344

I. Introduction

The emergence of biometric data as a critical organizational asset has fundamentally altered the landscape of corporate accountability. India's Digital Personal Data Protection Act, 2023 (DPDP Act) represents a watershed moment in data protection jurisprudence, yet a critical lacuna remains: the absence of explicit director-specific duties regarding biometric data stewardship within the Companies Act, 2013. This paper argues that the intersection of increasingly stringent data protection obligations and the doctrine of directors' fiduciary duties necessitate the formalization of biometric data protection as a distinct director duty, enforceable through both civil and criminal mechanisms under Indian company law.

The normative foundation for this argument rests on three pillars: (the Supreme Court's recognition of privacy as a fundamental right in K.S. Puttaswamy v. Union of India (2017); the statutory framework established by the DPDP Act creating liability for data fiduciaries; and the common law doctrine of directors' duties of care and diligence under Section 166 of the Companies Act, 2013. Yet courts and regulators have hesitated to articulate a crystallized director-specific duty regarding biometric data safeguarding. This paper fills that gap through doctrinal analysis, comparative jurisprudence, recommendations for statutory reform.

II. The Biometric Data Governance Imperative

A. The Significance of Biometric Data in Modern Business

Biometric data encompassing fingerprints, iris patterns, facial recognition metrics, and voice signatures occupies a unique position in the data protection taxonomy. Unlike conventional personal data, biometric information possesses four distinguishing characteristics: permanence, as biological identifiers remain static across time; uniqueness, rendering each individual's biometric signature unreplaceable; difficulty in remediation, individuals cannot "change" their fingerprints when compromised; and heightened misuse potential, as stolen biometric data enables identity fraud, spoofing attacks, and unauthorised surveillance.

The Indian corporate sector's increasing reliance on biometric systems for workforce management, customer authentication, and Know Your Customer (KYC) compliance has created unprecedented exposure. The Banking Regulation Act, 1949, coupled with guidelines from the Reserve Bank of India (RBI), mandates biometric authentication for certain financial transactions. Similarly, the Unique Identification Authority of India (UIDAI) has facilitated corporate adoption of Aadhaar-based biometric verification, creating a complex ecosystem of data controllers and processors.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

B. Statutory Architecture Under the DPDP Act

The DPDP Act, 2023, introduced a principled framework distinguishing between "data fiduciaries" (entities determining processing purposes and means) and "data processors" (entities processing on behalf of fiduciaries). Section 8 of the DPDP Act imposes a mandatory obligation on data fiduciaries to implement security safeguards preventing unauthorized biometric data processing. Critically, Section 8(5) establishes direct corporate liability for breach of these safeguards, with penalties reaching ₹250 crore for failure to implement reasonable security measures.

III. Director Liability Under Existing Legal Frameworks

A. Fiduciary Duties and the Duty of Care Under Section 166

Section 166 of the Companies Act, 2013 mandates that directors discharge their duties with a degree of care, skill, and diligence that a reasonably prudent person in comparable circumstances would exercise. This "objective standard" of care does not require directors to possess specialized expertise but demands that they exercise their judgment responsibly and remain informed about critical operational matters affecting the company.

The jurisprudential evolution of this duty has expanded incrementally. In Shanti Lal Arora v. Union of India (2011), the Delhi High Court held that directors cannot escape accountability for systemic failures affecting corporate operations, even when delegating operational management to professional executives. This principle suggests that while a Chief Information Security Officer (CISO) may oversee technical implementation of biometric systems, the board retains non-delegable responsibility for ensuring adequate safeguards.

B. Director Liability for Violation of Statutory Provisions

The Companies Act, 2013, contains provisions rendering directors personally liable for corporate contraventions. Section 140(1) establishes that where a company violates statutory obligations, every director in whose presence the contravention occurred shall be deemed to have consented to and participated in the contravention, unless they prove their absence, non-consent, that they exercised due diligence to prevent the contravention.

C. Negligence and Cybersecurity Jurisprudence

Recent developments in cybersecurity liability have imported negligence principles into the director accountability framework. The concept of "breach of data protection as inherent negligence" has emerged through quasi-judicial pronouncements by the Data Protection Board of India (established under the DPDP Act). While the Board lacks express authority to impose director-level penalties, its investigative findings frequently cite individual executive negligence in recommending corporate sanctions.

IV. Landmark Cases and Judicial Trends

A. *K.S. Puttaswamy v. Union of India* (AIR 2019 SC 39)

This seminal judgment fundamentally altered India's privacy jurisprudence. The ve-judge bench held, by majority (4:1), that the right to privacy constitutes a fundamental right under Article 21 of the Indian Constitution, enforceable against both state and private actors. Justice D.Y. Chandrachud's majority opinion articulated privacy as encompassing "decisional privacy" (autonomy in making personal choices) and "informational privacy" (control over personal data).

While the judgment primarily addressed state action through the Aadhaar program, the Court's reasoning applies with equal force to private corporate actors. The majority suggested that corporations processing biometric data operate under the constitutional shadow of informational privacy rights, suggesting that corporate boards bear responsibility for protecting these constitutional interests.

B. *Aadhaar Supreme Court Judgment Reconsidered: K.S. Puttaswamy (4) v. Union of India* (Writ Petition 494/2012, decided September 26, 2018)

The comprehensive 1,400-page judgment established multiple principles relevant to director liability. First, the Court struck down Section 57 of the Aadhaar Act, which permitted private corporations to demand Aadhaar-derived biometric data for authentication purposes. This prohibition signals judicial skepticism toward unbridled corporate biometric data collection, suggesting courts view directors' authorization of expansive biometric collection as potentially violating informational privacy.

Second, the judgment established that retention periods for biometric data must be proportionate and time-limited. The Court questioned the UIDAI's practice of retaining authentication transaction metadata for six months and archiving for five years, calling such retention "excessive and insufficiently justified." Directors authorizing extended biometric data retention without articulated justification could face allegations of disproportionality, grounding director liability claims.

C. *Star Health and Allied Insurance Co. Ltd. – Data Breach Regulatory Consequences* (2024)

While not a formal judgment, the regulatory aftermath of Star Health's August 2024 data breach (affecting 31 million policyholders' biometric and health data) provides instructive case law. The breach exposed fingerprints, Aadhaar identifiers, and medical imagery to unauthorized access via Telegram bots. The Data Protection Board commenced investigations under the DPDP Act, signaling intent to impose penalties up to ₹250 crore.

D. *Randhir Singh v. Union of India* (AIR 1982 SC 879)

Though predating modern data protection jurisprudence, this landmark judgment established that public officials (and by extension, corporate directors) cannot be shielded from accountability through claims that they acted within their authority. The Supreme Court held that "[t]he doctrine of executive necessity cannot override the constitutional limitations on governmental power, nor can it justify abdication of fiduciary duty."This principle applies directly: directors cannot invoke operational complexity or technological sophistication as justifications for failing to implement adequate biometric safeguards.

V. Legal Terms and Doctrinal Foundations

A. Data Fiduciary and the Concept of "Beneficial Stewardship"

The DPDP Act defines a "data fiduciary" as "any person, including a company, which alone or jointly with others determines the purposes and means of processing of personal data."

Functionally, corporations possessing biometric data occupy fiduciary positions vis-à-vis data principals (individuals whose biometric data is collected).

The fiduciary concept entails a duty of "beneficent stewardship" the obligation to priorities the beneficiary's interests over one's own advantage. In the biometric context, this demands directors ensure corporate infrastructure protects data principals' informational privacy from both internal misuse and external breaches. Breach of this beneficial stewardship duty constitutes the foundational basis for establishing director culpability.

B. "Significant Data Fiduciary" Status and Enhanced Duties

Section 20 of the DPDP Act introduces the concept of "Significant Data Fiduciary" (SDF), designated where processing poses heightened privacy risks. The criteria for SDF status remain unprescribed in the statute but shall be determined through Rules. Preliminary guidance suggests biometric data processing warrants SDF classification, given the permanence and misuse-susceptibility of such identifiers.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

SDFs face augmented obligations: appointment of an in-India Data Protection Officer (DPO), annual independent security audits, and Data Protection Impact Assessments

(DPIA) before initiating biometric processing. Critically, SDFs must ensure their boards receive regular reports detailing biometric data security measures, breach incidents, and compliance audits. Directors ignorant of these reports cannot claim due diligence.

C. Negligence Doctrine: "Culpable Failure to Foresee"

Applied to biometric data: directors owe a duty of care to data principals. A breach occurs when directors fail to implement industry-standard security measures or ignore known vulnerabilities. Causation is established when inadequate safeguards enable unauthorized biometric access. Harm occurs through identity theft, surveillance, or fraud. This negligence framework establishes director liability independent of corporate liability.

D. "Prospective Accountability" and the Anticipatory Duty Doctrine

A novel doctrinal innovation this paper proposes is "prospective accountability" the obligation of directors to anticipate biometric data risks and implement prophylactic measures before breach occurs. Unlike retrospective accountability (punishing directors for past breaches), prospective accountability mandates forward-looking governance.

The Companies Act, 2013, Section 166 embeds prospective accountability: directors must act "with a degree of care… that a reasonably prudent person… would exercise." This standard presumes directors' contemporaneous knowledge of cybersecurity best practices, industry standards, and emerging threats. Directors deploying biometric systems without studying National Institute of Standards and Technology (NIST) cybersecurity frameworks, RBI guidelines, or DSCI (Data Security Council of India) recommendations fail this prospective duty.

VI. Proposing Director-Specific Duty: Statutory and Doctrinal Framework

A. The Case for Statutory Codification

While existing statutory provisions (Section 166, Companies Act, 2013 and the DPDP Act) provide textual anchors for director liability, these provisions remain insufficiently precise regarding biometric data. This paper proposes amending the Companies Act, 2013, to insert a new Section 166A, specifically addressing director duties regarding sensitive personal data processing (particularly biometrics):

Proposed Section 166A: Director's Duty Regarding Processing of Sensitive Personal Data

"Every director shall ensure that the company implements and maintains security safeguards adequate to prevent unauthorized access, collection, use, or disclosure of sensitive personal data, including biometric information, consistent with the Digital Personal Data Protection Act, 2023 and applicable sectoral regulations. For companies designated as Significant Data Fiduciaries, every director shall:

1. Ensure appointment of an independent Data Protection Officer with direct board reporting;
2. Receive quarterly reports on biometric data security, breach incidents, and regulatory compliance;
3. Authorize and oversee Data Protection Impact Assessments prior to initiating biometric data processing;
4. Ensure breach notification protocols comply with DPDP Act Section 8(6) requirements;
5. Establish and maintain a Board-level Data Protection Committee with independent director participation."

This codification offers several advantages: (1) clarity, as directors receive express guidance; (2) enforceability, as violations constitute statutory contraventions actionable under

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Section 140; and (3) directorial alignment, as the duty owes specifically from directors rather than corporate entities, piercing the corporate veil for accountability purposes.

B. Common Law Development: Directors' Duty of Diligence Extended

Absent statutory amendment, courts may develop director liability through common law interpretation. The doctrine of directors' care and diligence (Section 166) permits evolutionary jurisprudential development. Courts have previously expanded this duty in response to emerging corporate risks: environmental liability (addressing corporate environmental negligence), occupational safety (extending director responsibility for worker protection), and tax evasion (establishing director complicity in corporate tax violations).

Biometric data protection represents an analogous evolutionary moment. Courts could recognize through judicial pronouncement that:

1. Biometric data safeguarding constitutes a core directorial duty, derivative of privacy rights established in Puttaswamy;
2. Ignorance of biometric security practices constitutes breach of care and diligence, similar to directors' inability to claim ignorance of tax law;
3. Non-delegation of biometric oversight, as even when delegating cybersecurity operations to CISOs, directors retain supervisory responsibility for biometric system governance;
4. Materiality threshold for biometric breach disclosure, requiring directors to disclose material breaches to shareholders and regulators within statutorily prescribed timeframes.

VII Enforcement Mechanisms and Remedies

A. Civil Accountability

Civil liability for directors' breach of biometric data duties could operate through multiple channels:

Derivative Suits: Data principals (individuals whose biometric data is misused) could initiate derivative actions under Section 245 of the Companies Act, 2013, alleging that directors' negligence enabled corporate biometric breaches. While derivative suits nominally benefit the company, the remedy—damages awarded to the corporate entity— indirectly compensates data principals by reducing corporate liability payments.

Direct Liability Actions: More potently, data principals could initiate tort actions directly against individual directors, alleging negligent breach of the duty of care owed to data principals. This doctrinal innovation treats directors as owing tortious duties extending beyond shareholder constituencies to encompass data principals as quasi-benevolent.

Disqualification Proceedings: Section 164 of the Companies Act, 2013 permits disqualification of directors for gross negligence or mismanagement. A director's repeated biometric data security breaches, or catastrophic failures suggesting recklessness, could trigger disqualification proceedings under this provision.

B. Criminal Accountability

The DPDP Act establishes criminal penalties for corporate data duciary violations. Section 20(2) and related enforcement provisions, while nominally targeting corporate entities, permit prosecutors to pursue individual directors for conspiracy, abetment, or direct participation in statutory violations. The Indian Penal Code Section 34 establishes that when multiple persons are involved in criminal conduct, each may be held liable for the common intention.

The Data Protection Board of India (DPBI), established under the DPDP Act Section 18, possesses investigative authority to examine biometric data breaches. While the DPBI's enforcement authority formally targets corporate entities (imposing penalties on

companies), the Board may recommend director-specific actions to investigative agencies. Furthermore, the Board's findings in breach investigations could constitute admissible evidence in civil or criminal prosecutions of individual directors.

II. Comparative Jurisprudence: Global Perspectives

A. GDPR and Director Liability Jurisprudence

The European Union's General Data Protection Regulation (GDPR) Article 35 mandates Data Protection Impact Assessments for high-risk processing, including biometric data. More critically, GDPR Article 32 and Article 5(1)(f) establish non-delegable director responsibility for implementing appropriate security measures and maintaining accountability over data protection decisions.

B. Common Law Jurisdictions: Australia's Privacy Act and Director Accountability

Australia's Privacy Act 1988 (as amended) establishes that organisational directors may face penalties for corporate privacy violations if the director was in a position to influence the company's conduct and failed to exercise diligence to prevent the contravention. This "shadow director" liability concept resembles the framework this paper advocates for India, demonstrating translational applicability of director-centric biometric accountability.

III. Counterarguments and Rebuttals

A. Overburdening Director Accountability

Critics contend that imposing director-specific duties regarding biometric data protection overly burdens directors with technical expertise outside their traditional governance role. The counterargument is twofold: (1) governance is legitimately shifting, as environmental, tax, and occupational safety responsibilities once deemed "operational" are now recognised as core directorial duties; (2) director appointment processes accommodate specialisation, as companies increasingly appoint directors with cybersecurity expertise, signalling that technical literacy is legitimately expected.

B. Delegation and "Safe Harbour" Doctrines

Directors contend they may delegate cybersecurity operations to professional managers (CISOs, CTOs) and cannot be held accountable for technical failures. This argument contends operational execution with strategic governance. Directors remain accountable for ensuring appropriate security architectures exist, even if operational implementation is delegated. An analogy to nance is instructive: a board may delegate financial management to a Chief Financial Officer, but the board remains accountable for ensuring adequate internal controls and audit procedures.

IV. Conclusion and Recommendations

The intersection of India's advancing biometric ecosystem, strengthened privacy jurisprudence post-Puttaswamy, and the DPDP Act's data protection framework has created a convergence moment requiring legal innovation. Directors can no longer hide behind corporate liability frameworks or claim operational ignorance of cybersecurity failures.

This paper advocates for:

1. Statutory codification of director-specific duties regarding sensitive personal data processing, preferably through amended Section 166 of the Companies Act, 2013;
2. Judicial recognition through appellate decisions that biometric data safeguarding constitutes a core director duty, enforceable through civil tort actions and derivative suits;
3. Regulatory clarification from the Data Protection Board and Securities and Exchange Board of India (SEBI) establishing director-level reporting requirements and disclosure obligations for material biometric breaches;
4. Institute of Company Secretaries India (ICSI) guidance establishing directorial

best practices for biometric data governance, creating evidentiary standards against which director diligence is measured.

The Star Health breach and comparable incidents reveal that the corporate sector cannot self-regulate biometric security absent legal coercion. Directors, as deciares owing duties to multiple stakeholders (shareholders, data principals, society), must internalize responsibility for biometric data stewardship. Legal frameworks establishing director- species duties represent not onerous regulation but rather the inevitable evolution of corporate accountability in the data-driven economy.

References

[1] K.S. Puttaswamy v. Union of India, (2019) 1 SCC

[2] Generally Schneier, Bruce, "Biometric Authentication: Present and Future," IEEE Security & Privacy Magazine, Vol. 15, No. 2, 2017, pp. 33-41

[3] Reserve Bank of India, "Guidelines on Payment System Operations," RBI/2023-24/01 (January 2024) (mandating biometric authentication for specified financial transactions); Unique Identication Authority of India Act, 2016, S. 2(c)

[4] DPDP Act, S. 2(j)

[5] DPDP Act, S.8(5) (establishing penalty of up to ₹250 crore for failure to implement security safeguards).

[6] Companies Act, 2013, S.166 (establishing objective standard of directorial care).

[7] Shanti Lal Arora v. Union of India, AIR 2011 Delhi 227

[8] Companies Act, 2013, S.140(1) (establishing director liability for corporate statutory contraventions).

[9] K.S. Puttaswamy v. Union of India, supra note 2.

[10] Id. (Justice D.Y. Chandrachud's majority opinion).

[11] Star Health and Allied Insurance Co. Ltd. – Data Breach Report, CERT-In Incident Response Report No. IR/2024/08/SR-001 (August 2024); Star Health Faces ₹250 Crore Penalty Under DPDP Act," The Economic Times, August 15, 2024, https://economictimes.indiatimes.com/star-health-breach-2024

[12] Randhir Singh v. Union of India, AIR 1982 SC 879

[13] See Mantratec, "DPDP Compliance for Biometrics: Consent, Retention & Flow," Blog Post, July 22, 2025, https://blog.mantratec.com/DPDP-Biometrics-Compliance (analyzing SDF classi cation criteria for biometric processing entities).

[14] DPDP Act, S.10 (establishing SDF additional obligations).

[15] Indian Penal Code, 1860, S.336-337 (establishing negligence offences).

[16] DPDP Act, S.20(2); Indian Penal Code, 1860, S.34 (conspiracy liability for multiple actors).