VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

SECURING THE DATA DELUGE: STATUTORY SECURITY OBLIGATIONS AND BREACH REGULATION FOR BIG DATA SYSTEMS IN INDIAN LAW

- Dr. Astitwa Bhargava[1] & Vemuru Leela Krishna[2]

ABSTRACT

Aggregation is itself a security risk. A big data repository is not simply a larger filing cabinet; it is a concentration of attack value, and every major Indian data breach of the last decade has exploited exactly that concentration. This paper maps the legal architecture that is supposed to secure such repositories: section 43A of the Information Technology Act and the SPDI Rules, the CERT-In reporting regime as tightened by the April 2022 Directions, and the security and breach-notification obligations of the Digital Personal Data Protection Act, 2023 read with the 2025 Rules. Measured against Articles 32 to 34 of the GDPR and the American breach-notification experience, the Indian framework emerges as newly strengthened on paper but fragmented in design: overlapping regulators, undefined standards of "reasonable security safeguards," a breach-notification duty unmoored from any risk threshold, and an adjudicatory body whose independence is doubtful. The paper argues that big data security regulation must shift from incident-reporting to architecture, and offers a set of doctrinally grounded suggestions to that end.

Keywords: Data Breach, CERT-In, Section 43A, DPDP Act 2023, Reasonable Security Safeguards, Breach Notification, Cybersecurity.

I. INTRODUCTION

Data protection law and data security law are usually taught as one subject, but they answer different questions. Data protection asks whether information *ought* to be processed; security asks whether, once processed, it can be *kept*. Indian scholarship has spent most of the

[1] Assistant Professor, National Law Institute University, Bhopal
[2] Research Scholar, National Law Institute University, Bhopal.

post-*Puttaswamy* decade on the first question.[3] The second has received less sustained attention, which is odd, because it is on the security side that Indian residents have been most visibly failed. The alleged exposure of some 81.5 crore records linked to the ICMR's COVID testing database in October 2023, the ransomware attack that crippled AIIMS Delhi for a fortnight in November 2022, and the 2021 MobiKwik incident involving data of roughly 3.5 crore users are only the incidents that reached the newspapers.[4] Each involved a large aggregated dataset. None resulted in compensation to a single affected individual.

This paper examines why. Part II makes the conceptual point that scale converts a privacy problem into a security problem. Parts III and IV set out the statutory architecture, before and after the Digital Personal Data Protection Act, 2023.[5] Part V draws comparisons with the GDPR and American law. Part VI identifies the structural gaps, and Part VII closes with suggestions. The method throughout is doctrinal; I am concerned with what the enacted texts require, permit and omit, not with compliance behaviour in the field.

II. THE SECURITY PROBLEM OF SCALE: AGGREGATION AS RISK

Security economics has a simple teaching: attackers allocate effort where the return is highest, and the return on a database grows super-linearly with its size and linkability. A repository holding identity, financial and health attributes for hundreds of millions of people is what the security literature calls a high-value target; in Schneier's phrase, data is a toxic asset, and hoarding it is hazardous in itself.[6] Justice Chandrachud's dissent in the Aadhaar case grasped the point juridically: centralised architecture creates a single point of failure, and the constitutional assessment of a data system must attend to its design, not merely to its stated purpose.[7]

---

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

[4] These incidents are drawn from contemporaneous reportage and CERT-In's public acknowledgements; in the ICMR matter, the agency confirmed investigation of the claimed sale of the dataset on a cybercrime forum in October 2023. Precise figures in breach reporting are, notoriously, contested, and are cited here as claimed rather than adjudicated.

[5] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].

[6] Bruce Schneier, *Data Is a Toxic Asset, So Why Not Throw It Out?*, CNN (Mar. 1, 2016); see generally BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 47–62 (2015).

[7] *Justice K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1 (India), at paras. 260–274 (Chandrachud, J., dissenting) [hereinafter *Puttaswamy II*].

Two legal consequences follow. First, security obligations cannot sensibly be uniform: the duty owed by the custodian of a national health database is not the duty owed by a neighbourhood e-commerce site, and a statute that speaks in one undifferentiated register has failed before enforcement begins. Second, breach harm in big data systems is probabilistic and delayed, identity fraud may follow months after exfiltration, which is precisely why compensation regimes keyed to proof of consequential loss systematically under-deter.[8]

III. THE ARCHITECTURE BEFORE 2023: SECTION 43A, THE SPDI RULES AND CERT-IN

Until 2023, the core civil obligation was section 43A of the Information Technology Act, 2000: a body corporate "possessing, dealing or handling any sensitive personal data" in a computer resource it owns, controls or operates, which is negligent in implementing "reasonable security practices and procedures" and thereby causes wrongful loss or wrongful gain, is liable to pay compensation.[9] The provision was fleshed out by the SPDI Rules of 2011, which defined sensitive personal data, prescribed consent and disclosure norms, and blessed IS/ISO/IEC 27001 as a deemed-compliant standard.[10]

Three defects made section 43A a paper tiger. It required proof of negligence *and* of wrongful loss or gain, a double hurdle in a domain where causation is diffuse. Its enforcement ran through adjudicating officers under section 46, a machinery that produced remarkably little reported jurisprudence in fifteen years. And it applied only to "body corporates," leaving the largest data repositories in the country, those of the state, entirely outside it. The criminal counterpart, section 72A on disclosure in breach of lawful contract, was narrower still.[11]

---

[8]For the American debate on standing and delayed breach harm, see *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), and *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), which together illustrate how demanding "concrete injury" requirements can leave breach victims remediless.

[9]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 43A, inserted by the Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

[10]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011) [hereinafter SPDI Rules], rr. 3, 8.

[11]The Information Technology Act, *supra* note 8, §§ 46, 72A. On the near-total absence of § 43A adjudication, see the Srikrishna Committee's assessment: COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS 6–9, 165–70 (2018).

The incident-response side belongs to CERT-In under section 70B. The Directions of 28 April 2022 transformed this regime: reporting of specified cyber incidents within *six hours* of noticing, mandatory time synchronisation with NIC/NPL servers, 180-day log retention within India, and extensive KYC and record-keeping duties for VPN, cloud and virtual asset providers.[12]The six-hour window is the most aggressive in the world, and that is not obviously a virtue. GDPR allows seventy-two hours to notify the supervisory authority precisely because early reports are unreliable; a six-hour clock produces defensive, content-free filings, and the Directions attach no publicity, no individual notification, and no remedial consequence to what is reported. Reporting, in this design, is intelligence collection for the state, not protection for the data principal.[13]

IV. SECURITY AND BREACH NOTIFICATION UNDER THE DPDP ACT, 2023 AND THE 2025 RULES

The DPDP Act addresses security in two short provisions. Section 8(5) obliges every data fiduciary to protect personal data in its possession or under its control, including data processed by a processor on its behalf, by taking "reasonable security safeguards to prevent personal data breach." Section 8(6) requires that, in the event of a breach, the fiduciary give intimation to the Data Protection Board *and each affected data principal*, in the prescribed form and manner.[14] The 2025 Rules give this operational shape: an immediate, concise notification to affected principals describing the breach, its likely consequences and the mitigation measures, and a fuller report to the Board, with updated particulars within seventy-two hours.[15] The penalty

[12]Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000, No. 20(3)/2022-CERT-In (Apr. 28, 2022); The Information Technology Act, *supra* note 8, § 70B(6).

[13]Compare Regulation (EU) 2016/679, art. 33(1), 2016 O.J. (L 119) 1 [hereinafter GDPR] (72 hours, "where feasible," with a risk threshold), with the CERT-In Directions, *supra* note 10 (six hours, no risk threshold, no individual notification).

[14]DPDP Act, *supra* note 4, §§ 8(5)–8(6). "Personal data breach" is defined in § 2(u) as any unauthorised processing or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access that compromises confidentiality, integrity or availability.

[15]Digital Personal Data Protection Rules, 2025 (notified November 2025), r. 6 (security safeguards, including encryption, access control, logs and back-ups) and r. 7 (breach intimation). The final Rules largely track the draft published for consultation in January 2025.

schedule is serious money at last: up to Rs. 250 crore for failure of security safeguards, and up to Rs. 200 crore for failure to notify.[16]

Two design choices deserve scrutiny. The first is the absence of any risk threshold for individual notification. Article 34 of the GDPR requires notice to data subjects only where the breach is "likely to result in a high risk" to them; the Indian provision requires intimation of *every* breach to *every* affected principal. That sounds protective, but universal notification is well documented to produce notice fatigue, and it gives fiduciaries a perverse incentive to construe "breach" narrowly at the threshold.[17] The second is the standardless standard. "Reasonable security safeguards" is defined nowhere in the Act; rule 6 supplies a list of minimum measures but no benchmark, no certification pathway, and no articulation of how reasonableness scales with volume and sensitivity. Fifteen years of section 43A should have taught the drafters that an undefined reasonableness duty, enforced by a body that must be moved into action, protects mostly the defendant.

There is also, now, a compensation vacuum. The 2023 Act repealed section 43A outright, and the Act itself confers no private right to compensation; penalties flow to the Consolidated Fund.[18] An affected data principal after November 2025 is thus, remarkably, in a *worse* remedial position than she was under the maligned section 43A, which at least contemplated compensation in terms.

V. COMPARATIVE STANDARDS: THE GDPR AND THE AMERICAN PATCHWORK

Article 32 of the GDPR ties the security obligation explicitly to "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing," and names pseudonymisation, encryption, resilience and regular testing as candidate measures.[19] The virtue of this drafting is not that it is precise, it is not, but that it is *scalar*: the duty rises with the risk, which is exactly the property a big data security norm requires. Articles 33 and 34 then split notification into a regulator-facing duty with a seventy-two hour outer limit and a subject-facing

[16]DPDP Act, *supra* note 4, § 33 read with the Schedule, entries 1–2.

[17]GDPR, *supra* note 11, art. 34(1). On notice fatigue in the American experience, see Fred H. Cate, *Information Security Breaches: Looking Back and Thinking Ahead* 5–7 (Ctr. for Info. Pol'y Leadership, 2008).

[18]DPDP Act, *supra* note 4, § 44(2) (omitting § 43A of the IT Act); § 34 (crediting penalties to the Consolidated Fund of India). The affected individual is left to the general law, and, where a state instrumentality is involved, to the constitutional remedy under Article 32 or 226.

[19]GDPR, *supra* note 11, art. 32(1).

duty gated by high risk. Enforcement practice has given the standard content; the Irish DPC's decisions against large platforms and the CJEU's clarification in *Víctor* that fear of misuse can itself ground non-material damage under Article 82 have together made security failure genuinely expensive in Europe.[20]

The United States, characteristically, regulates breach notification without regulating security, or did until recently. All fifty states have notification statutes, descended from California's pioneering 2002 law, but their thresholds, timelines and definitions diverge enough that multistate breaches trigger fifty-odd inconsistent duties.[21] Two federal developments matter for India. The SEC's 2023 rules requiring listed companies to disclose material cyber incidents within four business days show breach disclosure being repurposed as market regulation, an idea SEBI has partially mirrored through its 2023 amendments to the LODR framework.[22] And HIPAA's Security Rule demonstrates a workable middle path between vagueness and rigidity: required and addressable safeguards, scaled to entity size, with published audit protocols.[23]

VI. PERSISTENT GAPS: FRAGMENTATION, INDEPENDENCE AND THE MISSING ARCHITECTURE

Three structural problems survive the 2023 reform. The first is regulatory fragmentation. A single breach at a listed payment company today engages CERT-In (six-hour incident report), the Data Protection Board (breach intimation under section 8(6)), the RBI (cyber security framework and localisation directions for payment data),[24] SEBI (LODR disclosure), and sectoral regulators besides, with no statutory mechanism of coordination, no common taxonomy of

[20]Case C-340/21, *VB v. Natsionalnaagentsia za prihodite*, ECLI:EU:C:2023:986 (Dec. 14, 2023) (fear of future misuse following a breach may constitute non-material damage); GDPR, *supra* note 11, arts. 33–34, 82.

[21]CAL. CIV. CODE § 1798.82 (West 2023) (originally enacted as S.B. 1386, 2002). For the FTC's development of a de facto security standard through § 5 enforcement, see *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240–49 (3d Cir. 2015).

[22]Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023) (codified at 17 C.F.R. pts. 229, 232, 239, 240, 249); Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations, 2023, Gazette of India (June 14, 2023).

[23]45 C.F.R. §§ 164.302–.318 (2023).

[24]Reserve Bank of India, Storage of Payment System Data, DPSS.CO.OD No. 2785/06.08.005/2017-18 (Apr. 6, 2018); Reserve Bank of India, Cyber Security Framework in Banks, DBS.CO/CSITE/BC.11/33.01.001/2015-16 (June 2, 2016).

incidents, and no rule against inconsistent findings. Fragmentation of this kind is not merely untidy; it dilutes accountability, because every regulator can assume another is acting.

The second is the Data Protection Board itself. Its members are appointed by the Central Government on terms prescribed by the Central Government, and it functions "as an independent body" only by legislative assertion.[25] Since the Government is also the country's largest data fiduciary, and since section 17(2) permits blanket exemption of state instrumentalities by notification, the Board is asked to police its own architect. Whatever that arrangement is, it is not the "procedural guarantee against abuse" that *Puttaswamy* proportionality demands.[26]

The third gap is the absence of architectural regulation. Nothing in Indian law addresses the design questions that actually determine big data risk: whether datasets must be segmented, whether identifiers must be stored separately from attributes, whether federated or decentralised processing should be preferred for state databases, whether encryption at rest is mandatory for repositories above a threshold size. The 2025 Rules gesture at encryption and access control, but as minimum measures for all fiduciaries, not as graduated architecture duties for the largest ones. Security law in India remains a law of incidents. Big data requires a law of systems.

VII. SUGGESTIONS AND CONCLUSION

Six suggestions follow. *First*, "reasonable security safeguards" under section 8(5) should be given scalar content by rules or Board guidance on the Article 32 pattern: state of the art, cost, and the nature, scope and volume of processing, with published audit protocols for significant data fiduciaries. *Second*, individual breach notification should be gated by a risk threshold, while regulator notification remains universal; the present inversion serves nobody. *Third*, the six-hour CERT-In window should be harmonised with the seventy-two hour DPDP timeline through a single-portal filing that discharges both duties, so that fiduciaries report once, accurately, rather than thrice, defensively. *Fourth*, Parliament should restore a compensation remedy, whether as a statutory right before the Board or by directing a portion of penalties into a victim compensation fund; the repeal of section 43A without replacement is a plain regression. *Fifth*, the composition and tenure of the Data Protection Board must be insulated from the executive, on the selection-

[25]DPDP Act, *supra* note 4, §§ 18–23. The contrast with the Srikrishna Committee's recommendation of a selection committee anchored by the judiciary is stark. SRIKRISHNA COMMITTEE REPORT, *supra* note 9, at 152–58.

[26]*Puttaswamy*, *supra* note 2, at para. 180 (Chandrachud, J., plurality); DPDP Act, *supra* note 4, § 17(2)(a).

committee model the Srikrishna Committee proposed, if section 8(5) is ever to be enforced against the state. *Sixth*, for state-operated repositories above a prescribed scale, architectural requirements, segmentation, separation of identifiers, mandatory encryption at rest, and periodic third-party audit, should be statutory, not discretionary, giving legislative form to the warning in Justice Chandrachud's Aadhaar dissent.[27]

The conclusion can be brief. India has, in the space of three years, acquired the formal apparatus of a modern data security regime: statutory safeguards, universal breach notification, penalties large enough to be felt. What it has not acquired is a theory of scale. Until the intensity of the security obligation tracks the concentration of the data, the law will keep arriving after the breach, clipboard in hand, to count the records already gone.

[27] *Puttaswamy II*, *supra* note 6, at paras. 260–274 (Chandrachud, J., dissenting).