PUTTING THE DPDP ACT TO WORK: WHY INDIA'S DATA PROTECTION LAW STILL HAS GAPS TO CLOSE

Anshu Dagar*

ABSTRACT

India passed the Digital Personal Data Protection Act in August 2023, closing a gap that had existed in Indian law for years. There was simply no single statute telling companies what they could and could not do with a person's data. This paper looks beyond the text of the Act itself and asks a more practical question: is the law actually working as intended? Two and a half years on, several parts of the Act remain stuck in limbo; rules that were supposed to give the statute teeth have not been finalised, the regulator meant to enforce it is structured in a way that raises fair questions about its independence, and smaller businesses are left guessing at what compliance will eventually demand of them. Cross-border data transfer rules remain similarly undefined. This paper sets out these gaps one by one, places India's approach briefly alongside the European Union's GDPR, and closes with a set of concrete suggestions for what needs to happen before the Act can be said to genuinely protect the people it was written for.

Keywords: Data Protection, Privacy, Data Protection Board, India, GDPR, Compliance

SETTING THE SCENE

It took a nine-judge bench of the Supreme Court to settle a question that, in hindsight, seems obvious: that privacy is part of what Article 21 protects. That 2017 ruling is really where the story of this legislation begins. What followed was a long back-and-forth between committees, draft bills, industry lobbying, and public consultation, ending in a statute that looks quite different from where the conversation started. India's new privacy law is the country's first attempt at a single, cross-sector framework for how personal data may be collected, used, and stored, replacing the thin protections that used to sit inside the Information Technology Act, 2000.

*BA LLB, FIFTH YEAR, MVN UNIVERSITY, FARIDABAD, HARYANA.

To put the scale of this in perspective: India runs on digital transactions in a way few other countries do. Banking apps, UPI payments, Aadhaar-linked services, e-commerce, social media all of it generates a constant stream of financial, biometric, location, and behavioural data on hundreds of millions of people. For most of the last decade, that data moved around with almost no legal guardrails. If a company leaked your data or misused it, your options as an ordinary citizen were thin: a civil suit, mostly, which is slow and expensive and rarely worth pursuing over a data breach. This new framework was supposed to change that calculus by giving people actual, enforceable rights, and giving companies actual, enforceable duties.

What this paper does is fairly narrow in scope but, I think, useful: rather than simply summarising what the Act says (which plenty of commentary has already done), it tries to pin down where the implementation is falling short in practice, why that matters, how India's choices compare to the EU's GDPR, and what would need to change for the law to function as intended.

HOW WE GOT HERE?

Before 2023, the closest thing India had to a data protection law was Section 43A of the IT Act along with the 2011 Sensitive Personal Data Rules, both fairly thin instruments that applied only to "body corporates" and asked for nothing more specific than "reasonable security practices." No regulator, no defined rights, no penalty scheme that matched the scale of a real breach.

Puttaswamy changed the pressure on Parliament to act. The government set up the Justice B.N. Srikrishna Committee, which in 2018 produced a report "A Free and Fair Digital Economy" that became the skeleton of the first Personal Data Protection Bill. That bill, and a revised 2021 version, ran into heavy criticism: too much room carved out for government agencies to bypass the rules, data localisation requirements that industry said were unworkable, and a regulator (the proposed Data Protection Authority) whose independence was doubted from the start. Both versions were eventually pulled. What replaced them was a leaner, considerably simplified bill, most of the contentious localisation language gone, introduced afresh and passed by Parliament in August 2023. Six years, roughly, from the Srikrishna report to a functioning statute. That gap says something about how hard it is to balance an individual's privacy against a state that wants room to run surveillance and welfare programmes, and against businesses that did not want to be boxed in by rigid localisation rules.

WHAT THE ACT ACTUALLY SAYS?

Strip away the legal language and the core idea is simple: nobody should touch your data without asking first. The law calls the asker a "Data Fiduciary" and the person being asked a "Data Principal." Before any processing happens, the fiduciary needs clear, specific, informed permission, delivered through a notice written in plain language not buried in fine print that says exactly what's being collected and why. And permission isn't a one-time thing; a person can take it back whenever they want, though whatever happened before that point stays valid.

Section 7 carves out a set of "legitimate uses" where consent isn't required at all; think of situations like a person voluntarily handing over their data for a specific purpose, legal compliance, medical emergencies, or employment matters. Entities that the government designates as "Significant Data Fiduciaries" based on how much data they handle and how sensitive it is face extra obligations: periodic data protection impact assessments, independent audits, and an India-based data protection officer.

Individuals get a fairly generous set of tools: they can ask what data is held about them and who it's been passed along to, get it corrected or wiped, name someone to step in and exercise these rights on their behalf if they pass away or become incapacitated, and lodge a complaint if something goes wrong. There's also a new middleman role, a "Consent Manager", registered with the regulator that lets someone manage permissions across several fiduciaries from a single dashboard instead of dealing with each one separately. Watching over all of this is a dedicated authority empowered to investigate breaches and hand out penalties that can climb as high as two hundred and fifty crore rupees, with the amount tied to how bad and how prolonged the violation was.

WHERE THE IMPLEMENTATION IS STRUGGLING?

The Rules Aren't Finished: Parliament passed the DPDP Act in August 2023, but most of what actually makes it operational depends on rules the Central Government still has to notify. Draft rules only surfaced for public comment in January 2025, and at the time this is being written in mid-2026, some of the most important pieces the actual mechanics of cross-border transfers, how the regulator gets staffed and set up are still sitting unfinished. Everyone's stuck waiting: businesses can't lock down compliance programmes against a target that keeps moving, and citizens can't exercise rights that depend on machinery that hasn't been built yet.

Can the Board Really Act Independently: Earlier drafts of India's data protection law imagined an independent regulator. What actually got passed is a Board whose members are appointed, given tenure, and can be removed by the Central Government the same government that, through Section 17's broad exemptions, is itself one of the largest processors of personal data in the country. That's an awkward structural position for a regulator to be in: policing an entity that effectively controls its own leadership. There's also a fair question about capacity: whether a newly formed Board, however well-intentioned, has the technical depth to handle disputes involving large-scale breaches and complex data architectures at the volume India is likely to generate.

Small Businesses May Struggle to Keep Up: The Act does allow the government to carve out exemptions for certain categories of fiduciaries, startups among them, but exactly what those exemptions will look like is anyone's guess until the rules are finalised. In the meantime, a small business without a legal or compliance team is staring down the same consent-management, breach-notification, and grievance-redressal obligations as a large corporation with dedicated compliance staff. Unless the eventual rules build in some kind of graded, risk-based approach, there's a real risk that the Act ends up favouring incumbents simply because they can absorb the compliance cost more easily.

Cross-Border Transfer Rules Are Still Vague: Section 16 flips the earlier localisation logic on its head: data can move outside India freely unless the destination country is specifically restricted by the government. That's a friendlier approach for business than the older localisation-heavy drafts, but there's still no published restricted-country list, and no real guidance on what counts as an adequate safeguard for a transfer. For technology and outsourcing companies that move data across borders as a matter of routine, that's a meaningful gap, and there's no indication yet of how often such a list, once published, would even be updated.

Most People Don't Know These Rights Exist: One thing that gets lost in discussions about institutional design is the more basic problem of awareness. India's digital literacy varies enormously between cities and villages, and a right on paper does very little if the person it belongs to has never heard of it. Someone accessing digital banking through a correspondent in a small town, or interacting with a government scheme through a mobile app, is unlikely to know they can demand correction of their data or file a grievance, let alone have the means to pursue that grievance before a Board that will probably sit in a handful of major cities. None

of the institutional fixes discussed elsewhere in this paper means much without a parallel push on public awareness, in regional languages, through channels people actually use.

It Doesn't Always Fit Cleanly with Existing Sector Rules: Banking, securities, and insurance already run on their own data rules laid down separately by the RBI, SEBI, and IRDAI covering things like where data can be stored and what security standards apply. Nobody has yet spelt out how this new privacy framework is meant to sit alongside those older sectoral rules, so a bank or an insurer could plausibly end up facing two rulebooks that don't fully agree with each other. Until someone clarifies which framework wins out for a given category of data, regulated entities are basically left to work it out themselves.

LOOKING AT THE GDPR FOR COMPARISON

It's hard to talk about data protection law anywhere in the world without eventually comparing it to the EU's GDPR, which has become the default reference point. Brussels gives companies several lawful bases for processing data, legitimate interest and contractual necessity among them, while India leans almost entirely on consent, with only a narrow 'legitimate use' carve-out standing in for the rest. That keeps the compliance question simpler on the Indian side: no need to run the kind of balancing test a legitimate-interest claim demands under the European rules, but it also leaves less room to manoeuvre for routine, low-risk processing like internal analytics, and creates a temptation to lean too hard on broad consent clauses as a catch-all.

Europe also insists that each member state run its own independent supervisory authority, usually appointed through parliamentary or judicial channels built specifically to keep the executive branch at a distance a sharp contrast to how appointments work on the Indian side. Its rules set a hard seventy-two-hour clock for breach notification, where India has left the timeline to rules that still haven't landed. And on cross-border transfer adequacy decisions, standard contractual clauses, and binding corporate rules, the European system is far more developed than India's comparatively bare-bones blacklist approach. The Indian model may be easier to comply with straight out of the gate, but it gives up some of the certainty and independence built into its European counterpart, circling back to the concerns raised earlier in this paper.

WHAT WOULD ACTUALLY HELP?

A few things seem worth pushing for. The government should move faster on notifying the rules, particularly the ones governing cross-border transfer, breach notification timelines, and

how the Board gets constituted, because every month of delay is a month businesses spend building compliance programmes against guesswork.

The Board's appointment process could stand to be more transparent and less government-controlled; bringing in judicial or civil-society representation alongside government nominees would go some way toward addressing the independence question, especially given how often government bodies themselves process personal data.

A tiered, risk-based compliance framework with lighter obligations for smaller, lower-risk processors would stop the Act from accidentally punishing small businesses for lacking the resources of larger ones.

On cross-border transfers, clearer adequacy standards and a commitment to reviewing the restricted-country list on a regular schedule would give businesses something concrete to plan around.

And finally, real money and effort need to go into public awareness campaigns in regional languages, through channels beyond just English-language digital media so that the rights in this Act don't end up being exercised only by people who were already digitally literate and aware to begin with.

CLOSING THOUGHTS

This is a genuinely significant piece of legislation; it gives statutory form to a right that took a nine-judge bench of the Supreme Court to establish, and it arrives after nearly a decade of false starts. But any law is only as good as its implementation, and right now the implementation has real holes in it: rules still pending, a regulator whose independence is fairly questioned, compliance obligations that land harder on small businesses than large ones, and cross-border transfer provisions that remain more sketch than substance. None of that is fatal on its own, but closing these gaps with urgency, transparency, and genuine investment in public awareness is what will decide whether this framework actually protects the people it was written for, or just ends up as well-intentioned text sitting on a page.