

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

The Digital-Ecological Nexus: Evaluating Cyber Law, Data Protection, and Environmental Law in India's Reformative Era

AMIT SINGH SANDHU* AND VELICHETY MANIKHANTA SESA SAI ANIRUDHA**

ABSTRACT

The Indian legal landscape is navigating a dual transformation: the rapid digitisation of governance and an intensifying climate crisis. In the digital realm, the Digital Personal Data Protection Act, 2023 marks a fundamental shift from a consent-only regime to a framework built on Data Fiduciaries and Data Principals. As technology evolves toward decentralised systems and generative and agentic AI, however, the cyber-law framework of the Information Technology Act, 2000 faces an acute crisis of relevance, one that calls for a transition toward technological neutrality (future-proof drafting) and enhanced algorithmic clarity (AI made intelligible to humans). This paper critically evaluates the synergy between these digital frontiers and environmental law, a connection often overlooked in traditional legal discourse. It examines the ecological footprint of the digital economy, in particular the high energy consumption of data centres and the growing crisis of electronic waste, which poses a direct challenge to the constitutional guarantee of a healthy environment under Article 21. Against the backdrop of the National Education Policy 2020, the study advocates a multidisciplinary pedagogical shift that integrates green informatics into legal curricula, ensuring that future practitioners can navigate the intersection of data privacy and ecological sustainability. The paper further explores the need for legislative reforms that harmonise the requirements of the DPDP Act for data processing with environmental audits. It highlights how the integration of AI into judicial processes can streamline environmental litigation, provided such systems adhere to the principles of natural justice and preserve judicial discretion. Ultimately, the study calls for a phased, constitutionally aligned strategy that balances technological progress with constitutional morality, ensuring that India's digital sovereignty does not come at the cost of its environmental integrity.

Keywords: cyber law, DPDP Act 2023, environmental law, NEP 2020, data privacy, technological neutrality, green informatics, judicial efficiency, legislative reform

* Author is a Student at School of Law, Aurora Deemed to be University, Bhongir, Telangana, India.

** Author is a Student at School of Law, Aurora Deemed to be University, Bhongir, Telangana, India.

I. INTRODUCTION: A LAW FOR A DIFFERENT INTERNET

The Information Technology Act, 2000 was enacted to give legal recognition to electronic records and to make e-commerce workable within Indian law.¹ At the time, the digital environment it governed was built almost entirely of static web pages and simple relational databases, and its drafters could reasonably assume that a human being sat behind every transaction, someone whose intent, once formed, could in principle be traced. Two decades later, governance itself has moved online, and artificial-intelligence systems increasingly act not merely as tools but as intermediaries, and in some contexts as decision-makers in their own right. That founding assumption no longer holds, and the statute's silence on algorithmic accountability, transparency, and ethics has become one of the more consequential gaps in Indian technology law.

The argument proceeds as follows. Part II asks who answers for harm caused by an opaque algorithm, and whether Sections 43A and 72A of the IT Act can meaningfully assign that responsibility. Part III turns to the Digital Personal Data Protection Act, 2023, and to its attempt to replace a consent-only model with one built on fiduciary duty, as well as to the tension between that duty and the data-hungry nature of generative AI. Part IV asks a harder question: what legal status, if any, an autonomous 'agentic' system should hold. Part V argues for technology-neutral drafting that regulates outcomes rather than specific processes. Parts VI through VIII connect this discussion to a dimension rarely addressed in the same breath as AI regulation: the physical, energy-intensive infrastructure that makes any of it possible, and its implications under Article 21. Part IX sets out a reform agenda; Part X concludes.

II. ALGORITHMIC OPACITY AND THE LIMITS OF TRADITIONAL LIABILITY

A. The black-box problem

Contemporary AI systems, and large language models in particular, often reach conclusions through processes that resist reconstruction even by the engineers who built them. This is the phenomenon commonly described as 'black-box' logic: the system produces an output, but the reasoning that produced it cannot be fully retraced. That opacity sits uneasily alongside legal doctrines such as negligence, breach of statutory duty, and natural justice, each of which was built around the idea that a decision can, at least in principle, be explained and defended.

¹ The Information Technology Act, No. 21 of 2000, India Code (2000) [hereinafter IT Act].

B. Where sections 43A and 72A fall short

Two provisions of the IT Act are most often invoked when data-driven harm occurs. Section 43A creates a compensation liability for a body corporate that fails to maintain reasonable security practices while handling sensitive personal data;² Section 72A penalises disclosure of information obtained in breach of a lawful contract.³ Both provisions assume that a human actor's negligence, or a human actor's intent, can be located and traced. That assumption breaks down when an automated credit-scoring tool, or an AI system assisting a judicial or quasi-judicial process, produces a discriminatory or otherwise harmful result: it is frequently impossible to identify the 'intent' or 'knowledge' that Indian civil and criminal law ordinarily requires before liability can attach.

The difficulty is compounded by the fact that the first of those provisions is living on borrowed time. Section 44(2)(a) of the Digital Personal Data Protection Act, 2023 omits Section 43A from the IT Act altogether, and that sub-section has been notified to take effect on 13 May 2027; Section 43A therefore remains in force at the time of writing, but not for much longer.⁴ Section 72A survives untouched. The practical consequence is that the compensation route most often invoked for data-handling failures will close, and the statute that replaces it contains no provision addressed to algorithmic explanation at all.

C. Toward algorithmic clarity

If the principles of natural justice are to survive the shift to automated decision-making, an affected person must be able to understand, at least in outline, why a decision went against them. That requirement, what this article calls algorithmic clarity, is not yet a term of art in Indian law, but it captures what Sections 43A and 72A cannot deliver on their own: a standard that lets a court or tribunal test an algorithmic outcome the way it would test a human one.

III. FROM CONSENT TO FIDUCIARY DUTY: THE DPDP ACT'S RESPONSE

The Digital Personal Data Protection Act, 2023 marks a genuine break from the consent-only model of the IT Act era. Where earlier law treated a data-handling entity as a mere processor, the DPDP Act organises itself around the idea of a Data Fiduciary, an entity that determines the

² IT Act, § 43A.

³ *Id.* § 72A.

⁴ The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 44(2)(a) [hereinafter DPDP Act]. Sub-section 44(2) also omits § 87(2)(ob) of the IT Act, the rule-making power under which the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were framed. Sub-section 44(2) was notified to commence on 13 May 2027; § 43A and those Rules remain in force until that date.

purpose and means of processing personal data, whether alone or with others,⁵ and imposes on that entity an affirmative duty of care. The person to whom the data relates is, correspondingly, a Data Principal,⁶ and the Act extends that person's rights: a Data Fiduciary remains responsible for compliance even where processing has been outsourced to a Data Processor,⁷ the Central Government may designate high-volume or high-risk entities as Significant Data Fiduciaries subject to heightened obligations,⁸ and a Data Principal may seek correction or erasure of data no longer necessary for its original purpose, alongside a functioning grievance-redressal mechanism.⁹

That framework is, however, still largely prospective. The Act was brought into force by staggered commencement from 13 November 2025, and the operative provisions described above, Sections 3 to 17, take effect only on 13 May 2027; what is in force at present is essentially the institutional machinery of the Data Protection Board.¹⁰ The obligations discussed in this Part are therefore better read as the law that is about to govern than as the law that governs.

A. The minimisation problem

The data-minimisation principle of the Act, which confines consent, and so processing, to the personal data necessary for a specified purpose,¹¹ sits in direct tension with the way modern AI is actually built. Generative models improve by training on datasets that are large, often unstructured, and rarely collected with a single narrow purpose in mind. A regime that takes minimisation seriously and a technology that depends on scale cannot both be satisfied by the same set of rules; reconciling them will require either a narrower reading of 'necessary' for training data, or a distinct statutory carve-out subject to its own safeguards. Neither currently exists in Indian law.

IV. AGENTIC AI AND THE STRUGGLE FOR LEGAL PERSONHOOD

The IT Act recognises both digital signatures and electronic signatures,¹² but it does so on the premise that a signature, however affixed, is always wielded by a legal person: a human being or a corporation. 'Agentic' AI does not fit that premise. These are systems capable of setting

⁵ DPDP Act, § 2(i).

⁶ *Id.* § 2(j).

⁷ *Id.* § 8(1).

⁸ *Id.* § 10.

⁹ *Id.* §§ 12–13.

¹⁰ *Id.* §§ 3–17. On the staggered commencement notified on 13 November 2025, §§ 1(2), 2, 18–26, 35, 38–43 and 44(1) and (3) took effect at once; § 6(9) and § 27(1)(d) commence on 13 November 2026; and the remainder, including §§ 3 to 17, on 13 May 2027.

¹¹ *Id.* § 6(1) (requiring that consent 'be limited to such personal data as is necessary for such specified purpose'); see also *id.* § 8(7) (erasure once the specified purpose is no longer being served).

¹² IT Act, §§ 3, 3A, 5.

sub-goals and executing multi-step tasks across platforms with little or no contemporaneous human supervision, and current law has nothing to say about their status. If an autonomous agent enters into a contract, or does what Section 43 makes actionable as damage to a computer resource,¹³ the statute offers no answer to the basic question of who, or what, is liable. As these systems are drawn into judicial support roles or environmental-compliance audits, that vacuum becomes harder to ignore: some framework, whether through deemed agency, mandatory human sign-off, or a bespoke liability regime, will have to align their operation with constitutional morality and preserve the space for judicial discretion that automated efficiency tends to crowd out.

V. TECHNOLOGICAL NEUTRALITY AS A REFORM PRINCIPLE

Much of the IT Act's difficulty in the AI era traces back to its prescriptive character: it was drafted for the specific technologies available in 2000, not for the categories of technology that might follow. The centralised model of certification through a Controller of Certifying Authorities under Section 17¹⁴ illustrates the problem. It is a workable design for a centralised public-key infrastructure, but a poor fit for the decentralised architectures now emerging in Web3 and distributed AI systems, where no single certifying authority sits at the centre of the network.

The alternative is technological neutrality: legislation that regulates the outcomes of technology use (harm prevention, fairness, safety) rather than mandating particular encryption standards, storage architectures, or certification models. A future-proofed IT Act would specify what a system must not do, and leave how it is built to evolve.

VI. THE ENVIRONMENTAL DIMENSION: DATA INFRASTRUCTURE AND ARTICLE 21

A. Energy, water, and e-waste

The 'cloud' is a physical thing. Data centres are, functionally, the factories of the digital economy: they draw enormous amounts of electricity to run and cool servers, they strain local power grids that often still rely on non-renewable sources, and their cooling systems consume water that competes directly with the needs of surrounding communities. The hardware they house is also replaced on short cycles, and the resulting electronic waste, much of it improperly disposed of, introduces heavy-metal contamination into soil and water with direct consequences

¹³ *Id.* § 43.

¹⁴ *Id.* § 17.

for public health. That waste stream is separately regulated, through the E-Waste (Management) Rules, 2022, which superseded the 2016 Rules with effect from 1 April 2023 and place the cost of collection and disposal on producers through an extended producer responsibility regime.¹⁵ The point is not that the harm is unregulated, but that it is regulated somewhere else entirely: none of it registers in a statute concerned with data packets rather than power grids.

B. Article 21's textual reach

Article 21 guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law.¹⁶ The Supreme Court has long read that guarantee as extending well beyond mere physical survival to a life lived with dignity, and has specifically held that it includes the right to the enjoyment of pollution-free water and air.¹⁷ The Court's environmental jurisprudence more broadly rests on constitutional foundations laid in cases addressing industrial and environmental harm.¹⁸ If a data centre's water and energy draw, or the toxic residue of discarded hardware, causes the kind of environmental degradation those cases addressed, there is no obvious reason the constitutional analysis should differ merely because the harm originates in a server farm rather than a factory.

C. Harmonising DPDP audits with environmental law

One practical bridge already exists in the Significant Data Fiduciary category of the DPDP Act.¹⁹ Amending the criteria for that designation to include an entity's ecological footprint, and requiring an independent environmental audit alongside the annual data-protection audit, would harmonise the DPDP Act with the Environment (Protection) Act, 1986²⁰ without requiring an entirely new statutory framework. Publishing the resulting audit summaries would extend the idea of algorithmic clarity from the code itself to the physical cost of running it.

¹⁵ The E-Waste (Management) Rules, 2022, G.S.R. 801(E) (Nov. 2, 2022), Gazette of India, pt. II sec. 3(i), r. 1(2) (in force from 1 April 2023, in supersession of the E-Waste (Management) Rules, 2016), https://cpcb.nic.in/uploads/Projects/E-Waste/e-waste_rules_2022.pdf.

¹⁶ INDIA CONST. art. 21.

¹⁷ *Subhash Kumar v. State of Bihar*, AIR 1991 SC 420, (1991) 1 SCC 598 (holding that the right to live is a fundamental right under Article 21 and that it includes the right of enjoyment of pollution-free water and air for full enjoyment of life).

¹⁸ See *M.C. Mehta v. Union of India*, AIR 1987 SC 1086, (1987) 1 SCC 395 (holding an enterprise engaged in a hazardous or inherently dangerous activity strictly and absolutely liable for harm resulting from that activity, without the exceptions available under *Rylands v. Fletcher*). See generally M.P. JAIN, INDIAN CONSTITUTIONAL LAW (Justice Ruma Pal & Samaraditya Pal eds., 8th ed. 2018) (surveying the judicial expansion of Article 21 beyond mere physical existence).

¹⁹ DPDP Act, § 10.

²⁰ The Environment (Protection) Act, No. 29 of 1986, India Code (1986).

VII. JUDICIAL AI AND THE NATIONAL GREEN TRIBUNAL

The National Green Tribunal²¹ faces a caseload that increasingly involves satellite imagery of deforestation, air-quality time series, and toxic-waste tracking data. This is high-volume, pattern-heavy material that a purely human-led review process struggles to process quickly. AI tools purpose-built for it could meaningfully reduce backlog, but only if they remain assistive rather than determinative: the members of the Tribunal must retain final judicial discretion, and any party affected by an AI-assisted finding must be able to challenge the reasoning behind it. An AI system that identifies a pattern of violation offers a lead for a judge to investigate, not a verdict for a judge to rubber-stamp.

VIII. GREEN INFORMATICS AND LEGAL EDUCATION UNDER NEP 2020

The National Education Policy, 2020 calls for stand-alone legal universities to become multidisciplinary institutions, and for legal education itself to be informed by constitutional values and socio-cultural context rather than by black-letter rules alone.²² A lawyer who advises on data governance without any grasp of what that data actually costs to store and process is working with half the picture. A curriculum built around what this article terms green informatics, a deliberate pairing of data-privacy law with the energy and lifecycle costs of the infrastructure that law regulates, would produce practitioners equipped to handle the cases that Part VI describes: a Data Fiduciary's server farm causing measurable environmental harm, or an NGT matter that turns as much on technical energy data as on legal doctrine.

IX. RECOMMENDATIONS

Four reforms follow from the analysis above, and each can be implemented without a wholesale rewrite of existing statutes.

1. *Eco-data audits.* Amend the Significant Data Fiduciary criteria under the DPDP Act to include ecological footprint, and require carbon, energy-source, and water-usage reporting alongside existing data-protection audits.
2. *Assistive judicial AI.* Deploy AI tools to help the National Green Tribunal, and comparable tribunals, manage high-volume environmental data, subject to a firm rule that final findings remain a matter of human judicial discretion.

²¹ The National Green Tribunal Act, No. 19 of 2010, India Code (2010).

²² MINISTRY OF HUMAN RESOURCE DEVELOPMENT, GOVERNMENT OF INDIA, *National Education Policy 2020*, ¶¶ 20.2, 20.4, at 50 (2020), https://ncert.nic.in/pdf/nep/NEP_2020.pdf.

3. *Technology-neutral drafting.* Amend the IT Act to regulate outcomes, that is, harm prevention, fairness and transparency, rather than prescribing specific technical processes that decentralised and agentic systems will inevitably outgrow.
4. *Green informatics in legal education.* Build the energy and lifecycle costs of data infrastructure into cyber-law and data-protection curricula, consistent with the multidisciplinary mandate of NEP 2020.

X. CONCLUSION

The IT Act, 2000 was not written for a world of autonomous agents, generative models, or data centres large enough to strain a regional power grid. Patching individual provisions, a redefined Section 17 here, a successor to the soon-to-be-omitted Section 43A there, will not close that gap on its own. What is needed is a shift in drafting philosophy, from rules tied to the technology of a particular year toward standards tied to outcomes that can survive the next one, paired with an honest reckoning that every byte processed under the DPDP Act has a physical cost that Article 21 already has the doctrinal tools to address. Digital sovereignty and environmental integrity are not competing goals; a legal framework that treats them as such will eventually have to answer for both.
