Page 4069 - 4087 **DOI:** *https://doij.org/10.10000/IJLMH.1111988*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

From Code to Court: Measuring the Regulatory Gap between Emerging Technologies and Existing Legal Structures - An Empirical Study

VISHVENDRA RAJ MALIK[1]

ABSTRACT

As technological change crosses a certain threshold and ceases to be disruptive, it becomes constitutionally valuable. The collection of advances in artificial intelligence/big data analytics/drone technology/algorithmic decision-making/digital surveillance has led to a growing gulf between machines can do today and what the law has any agreed-upon answer for. This article therefore studies that chasm which I term the regulatory gap as it is emergent within the Indian legal order, mapping how the deployment of new technologies at a rapid pace has quickly outpaced efforts to adapt existing statutory and constitutional regimes. Based on legislative trends, judicial pronouncements and comparative regulatory experience, the analysis argues that Articles 14, 19, and 21 of the Indian Constitution already provide about the normative tools for filling this lacuna sufficient purposive application by courts and legislatures willing to imagine. This paper critically examines the landmark 2023 legislative package passed in India which includes, inter alia, the "Digital Personal Data Protection Act", the three new criminal codes enacted under a Preamble frames approach to lawmaking ("the Criminal Procedure Code; the Indian Penal Code & the Indian Evidence Act"), along with other recent legislation such as that through which it amended its Competition Act and Telecommunications Act in nanoseconds but not others. This central finding is sobering: far from the type of routine administrative concern that one would imagine, the regulatory gap represents at best a slow-moving constitutional crisis, one that will require a multi-stakeholder, rights-anchored governance architecture to remediate before the damage becomes irreversible.

Keywords: *Regulatory Gap, Emerging Technologies, Artificial Intelligence, Digital Personal Data Protection Act 2023, Constitutional Law, Algorithmic Governance, Bharatiya Nyaya Sanhita, Surveillance, Competition Law, Technological Governance*

[1] Author is an Assistant Professor at IIMT University, Meerut, Uttar Pradesh, India.

 [ISSN 2581-5369]

I. INTRODUCTION

In the twenty-first century, the relationship between law and technology has gone awry. Machines are more powerful now, but that is not all there is to the story. The aspect of it is that the pace of technological change has shattered the normal rhythms by which legal systems take in novelty. Bail, credit score, election campaign and medical diagnosis are just some examples of decisions now influenced by algorithms. Some facial recognition tools are scanning crowds without any statutory authorisation. Predictive policing systems give risk scores to people who have not committed an offence. Plus, most of the laws that insist on governing all this were penned for a world that had none of it.[2]

The narrow regulatory gap referred to in this paper is not just an empty set of words, but a specific and measurable distance between the legality or capacity and the functionality or use of a technology on one side, as compared with the calibration of legal rules governing that technology on another. The notion was gradually and systematically theorised in the literature on algorithmic systems, which noted how automated decision-making has a complexity and opacity dimension that makes traditional rules of evidence, liability and constitutional due process functionally defunct.[3] That diagnosis, previously confined to academic journals only, has now been turned into operational reality. Klaus Schwab describes the Fourth Industrial Revolution as a transformative era which brings together three different systems through its technological advancements. He asserts that the revolution will bring about complete transformations of our daily existence and work methods while it will create economic and industrial and human understanding transformations. The revolution is powered by artificial intelligence and nanotechnology and 3D printing which are transforming multiple industries while they create new challenges for current business practices. Schwab wants technology to build human capacity and drive social development in the future while he asks all people to work together in their shared duty of protecting shared welfare.

Of all countries, India, in many ways is the most interesting to study this phenomenon. There are 750 million internet users, a rapidly growing AI sector, and a history of constitutional law that has shown an unexpectedly creative ability to accommodate new claims of rights so India is almost tailor made to make the question of regulatory gaps in the face of fundamental rights weighty national business. The Government has written in public that artificial intelligence is a

[2] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019) 15.
[3] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 3.

 [ISSN 2581-5369]

transformational national priority and this was done by NITI Aayog.[4] But the legislative response has been uneven. However, "the Digital Personal Data Protection Act 2023" has been long overdue and welcome in broad terms, albeit with narrow coverage. While the "Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam" together are arguably also one of India lately most complete endeavours at revising core criminal law post-1947, a fair deal of questions exists for technology specific contexts that remain unanswered. Model competition framework updated but does not reflect those forums and struggles with distinguishing mechanics of platform dominance.[5]

The structure of this paper is as follows: The following section, Part II builds the empirical and theoretical foundation for quantifying the regulatory gap. Part III explores the constitutional underpinnings that any sensible regulatory response would have to have. Parts IV- VI tackle the three areas where this disparity is most pronounced: criminal justice, including electronic evidence; privacy-related data governance; and competition law in the digital economy. Part VII provides conclusions, and prescriptive suggestions for reform based on constitutional principle rather than technocratic preference.

II. THEORETICAL AND METHODOLOGICAL FRAMEWORK: MEASURING THE REGULATORY GAP

Regulatory gap is not an on-off switch. It occupies a spectrum. Filling in the blanks at one extreme need nothing more than a little judicial creativity mending a court's definitions of statutes here and there, pushing a doctrine well-known into more unfamiliar facts. At the other end exist structural vacuums; entire categories of technological activity for which no cognizable legal framework is at all existent. Any serious attempt to study the gap must distinguish between these conditions, which in turn requires a theoretical framework that integrates constitutional doctrine, regulatory theory, and empirical legal methods.

The starting point, in the Indian context, is the landmark judgement Justice K.S. Puttaswamy v Union of India,[6] the landmark judgement which comprises 9 judges bench held that the right to privacy as a fundamental right under Article 21. Beyond its doctrinal holding, what is important for this study about Puttaswamy At bottom, the case represents judicial acknowledgment that constitutional meaning cannot be petrified in 1950. The concurring verdict of Justice D. Y. Chandrachud articulated an affirmative dimension to the guarantee — that while informational

[4] Ministry of Electronics and Information Technology (MeitY), *National Strategy for Artificial Intelligence* (Government of India 2018) 5.
[5] The Digital Personal Data Protection Act 2023 (Act 22 of 2023).
[6] *Puttaswamy v Union of India* AIR 2017 SC 4161.

 [ISSN 2581-5369]

privacy shall not be violated by the state, it must also positively protect such privacy via legislation. That positive dimension created a constitutional demand for data protection law, a demand that went unmet for six years.

Jack Balkin has identified the fundamental reason behind the regulatory gap through a time-based analysis which shows that democratic lawmaking requires extended discussion while technological deployment happens without delay.[7] The gap consists of three analytical components which Gary Marchetti identifies as definitional deficit which represents laws that lack adequate definitions of new technologies and structural deficit which describes regulatory institutions that are unfit for technical oversight and remedial deficit which denotes the absence of meaningful enforcement mechanisms.[8] The research paper uses Marchetti's three-part framework as its foundation but introduces an additional element specifically designed to address the requirements of Indian constitutional law through the constitutional accountability deficit which describes the lack of systems that would prevent technological power from violating fundamental rights protections established in Part III.[9]

The empirical methodology combines doctrinal legal analysis with what the paper terms ‘regulatory mapping’. The process of doctrinal analysis requires researchers to conduct systematic investigations of constitutional provisions, statutory texts, subordinate legislation, and judicial decisions. Regulatory mapping identifies particular technological fields, which include artificial intelligence and digital surveillance and platform economies and electronic evidence, to evaluate whether current legal systems properly handle each area. The study produces an Empirical Regulatory Gap Matrix which evaluates four dimensions: definitional adequacy and institutional capacity and remedial effectiveness and constitutional accountability.

III. CONSTITUTIONAL FOUNDATIONS FOR TECHNOLOGY GOVERNANCE: PRINCIPLES AND PRECEPTS

A. The Right to Privacy as Constitutional Bedrock

India's relationship with technology through its constitutional system begins and returns to Puttaswamy.[10] The nine-judge bench reached a landmark decision declared that privacy exists as a fundamental right of the human dignity which people possess under Article 21. The six

[7] Jack Balkin, 'The Three Laws of Robotics in the Age of Big Data' (2017) 78 *Ohio State Law Journal* 1217, 1220.
[8] Gary Marchetti, 'AI Regulation: A Practical Guide to Emerging Frameworks' (2022) 34 *Harvard Journal of Law and Technology* 189, 193.
[9] Constitution of India 1950, art 21.
[10] *Puttaswamy v Union of India* AIR 2017 SC 4161.

 [ISSN 2581-5369]

concurring opinions used the constitutional reading method which requires judges to interpret constitutional texts according to their contemporary operating conditions present at their time of enactment. Justice Chandrachud's ruling evaluates privacy rights through his definition of informational privacy which serves as the core element of his judgment. He views it as a mechanism that grants individuals the right to manage the dissemination of their personal data which he considers a constitutional right that includes both negative and positive aspects. The state requires protection against privacy invasions because the government must establish laws which enable people to use their privacy rights. The six-year period after Puttaswamy remained without legislative action because it represented a policy failure and a constitutional violation.

The court established a proportionality standard which evaluates state actions that affect privacy rights through the combined functioning of Articles 14 and 21. The standard requires four elements which state that an action needs to achieve a legitimate purpose while the action must show a logical relationship to the established goal through its use of the least severe options that protect privacy rights according to the standard. The four-part test, recognized within the general framework of European constitutional traditions, has become the fundamental standard for evaluating all technology-related laws in India. The legal system requires judges to handle technical details because this process is necessary for correct system operation, yet this requirement creates its own distinct difficulties.

B. Digital Surveillance and the Limits of State Power

The Supreme Court in the case of Anuradha Bhasin v Union of India,[11] demonstrated how digital surveillance operations impact constitutional rights when the Court evaluated India's prolonged communication suspension in Jammu and Kashmir after the region lost its special constitutional privileges. The Court established three fundamental rules when it decided that internet access forms part of Article 19 rights and internet shutdowns need proportionality testing and executive orders that ban digital communication services must undergo judicial assessment. The Apex Court in the case of Foundation for Media Professionals v UT of Jammu & Kashmir[12] reinforced this point, insisting that restrictions on the digital communications must be time-bound and they are strictly proportionate.

The state faces direct adverse consequences from the doctrinal consequences that AI-powered surveillance systems impose on its operations. The targeted use of facial recognition systems and predictive policing algorithms and mass data harvesting tools requires a higher standard of

[11] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.
[12] *Foundation for Media Professionals v UT of Jammu & Kashmir* (2020) 5 SCC 746.

 [ISSN 2581-5369]

constitutional justification because internet shutdowns need such justification according to the law. The Court's ruling in re: Pegasus Project[13] brought out the full meaning of this situation. The Court created a technical expert committee to investigate allegations that commercial spyware had been used against journalists and lawyers and civil society members in India while it denied the Indian government the right to use national security as unlimited reason for hiding information from the public. The decision establishes that the constitutional right against surveillance does not carry a technology exemption: what the state may not do through a warrant, it may not do through an algorithm.

IV. ELECTRONIC EVIDENCE, ALGORITHMIC PROOF, AND THE NEW CRIMINAL CODES

The criminal justice system shows direct effects from all regulatory gaps which exist in various domains. The prosecution needs to establish digital evidence as admissible before a conviction can proceed. The reliability of an algorithmic risk assessment shapes whether an accused obtains bail. The forensic integrity of data from cloud platforms or IoT devices establishes whether guilt or innocence can be proved. The 2023 legislative transformation of India's criminal law framework offers a convenient moment to assess how much of this gap has been closed — and how much has not.

A. The Pre-Reform Landscape: Sections 65A and 65B of the Indian Evidence Act

The two major provision of the Indian Evidence Act 1872[14] which were established in 1872 to govern electronic record admission standards failed to operate correctly for almost twenty years. The Court fought over the Section 65B certification procedure which created continuous conflicts among judicial authorities. The Supreme Court established in the case of Anvar P.V. v P.K. Basheer,[15] that Section 65B certification served as essential requirement for electronic record secondary admission thus overturning previous legal decisions which allowed different evidence methods. The situation created severe operational challenges because people could not access original documents or certifying officials. The Court established rules for certificate demand but in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal[16] the court failed to resolve the core dispute between the two parties. The traditional digital evidence system already faced challenges but the system lacked proper preparation for evidence demands which emerged from cloud computing and distributed ledger technology and AI-generated materials.

[13] *In re: Pegasus Project* (2022) 9 SCC 1.
[14] The Indian Evidence Act 1872 (Act 1 of 1872), ss 65A–65B.
[15] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473.
[16] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

 [ISSN 2581-5369]

B. The Bharatiya Sakshya Adhiniyam 2023: Reform and Residual Gaps

The Bharatiya Sakshya Adhiniyam 2023 (BSA)[17] carries forward the Section 65B architecture which now exists in Section 63 through its specific changes. The definitional expansion to cover data generated or stored in any electronic form represents a genuine improvement because it enables the evidentiary system to include cloud-stored and IoT-generated records. The extension of electronic records provisions to quasi-judicial and administrative proceedings partially addresses the concerns the Court had raised in the case of Shafi Mohammad v State of Himachal Pradesh.[18] These are not trivial advances.

What the BSA does not address, however, is the evidentiary universe that matters most going forward. How should an Indian court assess the reliability of AI-generated content tendered as evidence? What authentication requirements apply when the record-generating system is itself a machine-learning model rather than a human operator? What foundation must the prosecution lay before a facial recognition match or a predictive risk score is placed before a jury? What obligations of disclosure attach to the training data and documented error rates of an algorithmic tool used in prosecution? The questions lack statutory responses which creates constitutional importance through the resulting silent response. The right to fair trial under Article 21 interpreted through the lens of Chandrachud J.'s jurisprudence as a substantive rather than merely procedural guarantee necessarily includes the right to meaningfully contest evidence generated by automated systems. The right becomes empty without showing system operation details and information about its failure rates.

C. The Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita: Cybercrime and Procedural Dimensions

The Bharatiya Nyaya Sanhita 2023 (BNS)[19] and the Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS)[20] are ambitious instruments. The BNS consolidates previously fragmented offences relating to organised crime, terrorism, and state-hostile communications, and Section 111's treatment of organised crime alongside Section 152's provisions on threats to national integrity[21] mark genuine improvements in statutory coherence. The BNSS introduces welcome procedural modernisation: electronic summons, digital filing, and video-examined witnesses are now statutory options rather than ad hoc accommodations.

[17] The Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023).
[18] *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.
[19] The Bharatiya Nyaya Sanhita 2023 (Act 45 of 2023).
[20] The Bharatiya Nagarik Suraksha Sanhita 2023 (Act 46 of 2023).
[21] The Bharatiya Nyaya Sanhita 2023 (Act 45 of 2023), s 111 (organized crime); s 152 (acts endangering sovereignty).

 [ISSN 2581-5369]

The silences, however, are telling. The new codes say nothing about the criminal liability of AI system operators for autonomous decisions that produce harmful outcomes. They do not resolve the jurisdictional tangle that arises when a cybercrime is planned in one country and the same is executed through infrastructure in a second, and felt in a third. Encrypted communications the evidentiary challenge that frustrates criminal investigation more than any other receive no treatment. Neither does the misuse of AI for fraud, impersonation, or coordinated deception, an omission whose significance grows by the day. The principles governing inherent criminal jurisdiction developed in State of Haryana v Bhajan Lal,[22] and the protections surrounding investigative process articulated in Ram Jethmalani v Union of India[23] and Yashwant Sinha v CBI[24] offer useful frameworks for judicial intervention in technology-related criminal disputes, but they cannot substitute for legislative clarity on questions that Parliament has declined to confront.

V. DATA PROTECTION, PRIVACY GOVERNANCE, AND THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 (DPDPA)[25] which became law in 2023 was recognized as a significant legal achievement by the public who had expected its official implementation. The DPDPA marks the first time Parliament declared informational privacy as a legally protected right after the Supreme Court ordered complete data protection laws six years earlier in the Puttaswamy judgment. The Act establishes a modern data protection law structure which includes advanced elements that meet current standards. The statute analysis shows that it establishes the basic requirements for data protection yet fails to provide complete regulatory coverage of its established rules.

A. Core Architecture of the DPDPA

The DPDPA's framework centres on consent[26] as the lawful basis for personal data processing, together with rights of access, correction, and erasure for data principals, enhanced protections for children's data, and the creation of a Data Protection Board of India as the primary enforcement body. The Act draws recognisably from the European General Data Protection Regulation's[27] conceptual framework — particularly its insistence on purpose limitation and

[22] *State of Haryana v Bhajan Lal* AIR 1992 SC 604.
[23] *Ram Jethmalani v Union of India* (2011) 8 SCC 1.
[24] *Yashwant Sinha v CBI* (2019) 6 SCC 1.
[25] The Digital Personal Data Protection Act 2023 (Act 22 of 2023).
[26] The Digital Personal Data Protection Act 2023 (Act 22 of 2023), s 4.
[27] European Parliament and Council Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 22.

 [ISSN 2581-5369]

explicit consent — while adapting these ideas to Indian administrative realities. The data processor's fiduciary duties should be evaluated through the lens of Indian trust law because this framework establishes a relationship-based responsibility that goes beyond simple legal obligations. The consent mechanism, however, has attracted legitimate criticism. A country with major digital literacy disparities between different social and economic groups will find its users facing genuine informed decision-making obstacles because platform design teams create their systems to prevent users from making fully informed decisions. The DPDPA enforcement system lacks the capacity to identify actual consent because it handles form completion without understanding its implications as a valid form of consent.

B. The Aadhaar Precedent and Informational Sovereignty

The Aadhaar litigation is essential for understanding the constitutional framework that supports the DPDPA. The Apex Court in the landmark judement of K.S. Puttaswamy v Union of India ,[28] trying to maintained the fundamental structure of the Aadhaar card (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016[29] while declaring that its Aadhaar-based authentication systems for private organizations represented excessive breaches of individual privacy rights. The majority opinion established that law enforcement agencies need to provide a strong reason to collect biometric information because the biometric data should be treated as highly confidential personal data that requires extra protective measures. Justice Chandrachud's dissent went considerably further, characterising the Aadhaar infrastructure as a centralised surveillance architecture which fundamentally conflicts with the principles of constitutional democracy.

The dissenting opinion made a permanent impact on the field by defining the term 'data colonialism' which describes how governments and businesses take personal data from people while preventing them from retaining control over their own information. The majority did not use this framing but it has influenced academic analysis in the field and it has established two fundamental principles of data protection through the DPDPA which creates mandatory rules for public and private organizations to follow when handling data.

C. Algorithmic Accountability and the DPDPA's Silences

The DPDPA has a major shortcoming because it does not regulate automated decision-making. The law lacks regulations for automated decision-making which exist in Article 22 of the

[28] *Puttaswamy v Union of India* (2019) 1 SCC 1 .

[29] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Act 18 of 2016).

 [ISSN 2581-5369]

GDPR.,[30] automated decisions that produce considerable legal or financial ramifications on anyone. In contemporary India, algorithmic systems already influence credit approvals, insurance pricing, public benefit eligibility determinations, and in some jurisdictions bail assessments. To process those decisions without any right of explanation or contestation is to allow a form of automated arbitrariness that sits uneasily with Article 14's insistence on reasoned, non-arbitrary state action.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021[31] introduced some transparency obligations for significant social media intermediaries regarding content moderation, but their scope is narrow and their application to automated decision-making in other contexts is doubtful. The constitutional principle most relevant here is that which emerges from Shreya Singhal v Union of India[32] The Constitution establishes that fundamental rights cannot be violated through technological exceptions. An algorithmic execution of a state action which would raise constitutional doubts if performed by a human officer acquires no legitimate status. The DPDPA interpretation together with forthcoming AI governance laws must follow that guiding principle.

VI. COMPETITION LAW, PLATFORM DOMINANCE, AND THE REGULATORY CHALLENGE OF THE DIGITAL ECONOMY

The digital economy has produced forms of market power that the architects of competition law did not anticipate. The combination of network effects and proprietary data advantages and platform architecture design creates conditions that lead to market dominance which cannot be eliminated by standard antitrust solutions. The constitutional right which provides to carry on any trade or profession under Article 19(1)(g), read with the state's regulatory authority under Article 19(6), provides the normative foundation for competition regulation, but whether that foundation supports the kind of regulation that digital markets actually require depends on the adequacy of the Competition Act 2002 and its 2023 amendment.

A. The Competition Commission of India and Digital Markets

The Section 4 of the Competition Act 2002[33] which prohibits dominant firms from engaging in such practices that foreclose competition, impose unfair conditions, or deny market access. The Competition Commission of India (CCI) has applied this provision to digital platforms with growing confidence and, ultimately, considerable consequence. The most significant decision

[30] GDPR (n 31), art 22.
[31] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4(2).
[32] *Shreya Singhal v Union of India* AIR 2015 SC 1523.
[33] The Competition Act 2002 (Act 12 of 2003), s 4.

 [ISSN 2581-5369]

in this line is Competition Commission of India v Google LLC,[34] under this case The CCI conducted a lengthy investigation before it and imposed a penalty of Rs. 1,337.76 crore on Google for its market dominance which extended across web search and mobile operating systems and app distribution and video hosting services. The court issued two types of penalties to Google which included financial damages and required Google to implement interoperability functions for Android devices. The decision marks the first time in the Indian competition law has been applied to a major digital platform while the CCI shows its improved ability to analyse competition cases. Telefonaktiebolaget LM Ericsson v Competition Commission of India[35] added a related doctrinal contribution, confirming that the assertion of standard-essential patents in the technology sector is not, without more, insulated from competition scrutiny.

The Competition (Amendment) Act 2023[36] introduced deal value thresholds for merger notifications — a direct response to the phenomenon of acquisitions of data-rich startups that fall below conventional turnover thresholds while raising serious competitive concerns — and strengthened the framework for addressing anti-competitive digital conduct. The CCI's subsequent order in Google (Case No 39 of 2018)[37] further refined the regulatory approach to app store practices. Taken together, these developments suggest a credible and accelerating regulatory engagement with platform power, even if the pace of regulatory adaptation continues to trail the speed of market evolution.

B. The Global Context and India's Regulatory Positioning

The regulation of platforms exists as a global issue because domestic competition law cannot completely solve this problem. Indian policymakers need to understand the different regulatory approaches which the US Department of Justice antitrust case against Google[38] and the EU Digital Markets Act and Digital Services Act[39] establish. The Digital Markets Act which the EU establishes through its Digital Markets Act creates specific obligations for certain gatekeepers instead of using the more gradual approach which ex post investigation and enforcement require. The 2023 Amendment establishes only partial answers to the question of whether India should adopt a regulatory system which applies different rules than the Competition Act framework.

[34] *Competition Commission of India v Google LLC* 2023 CCI Order (Competition Commission of India, Case No 7 of 2012).
[35] *Telefonaktiebolaget LM Ericsson v Competition Commission of India* (2016) DELHC 2114.
[36] Competition (Amendment) Act 2023 (Act 18 of 2023).
[37] *Competition Commission of India v Google LLC*, Case No 39 of 2018 (Competition Commission of India 2022), affirmed on merits.
[38] *United States v Google LLC*, No 1:20-cv-03010 (US District Court, DDC 2023).
[39] Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1.

 [ISSN 2581-5369]

India needs to make real choices about its digital economy through its regulations because they will determine how the country operates. India needs to establish domestic capacity through its investment in regulated industries but excessive ex ante regulations will prevent this goal. The constitutional framework determines the boundaries for how the two parties need to negotiate their trade-off solutions. The Supreme Court requires all trade-off decisions between Shyam Telecom Ltd v BSNL[40] through Article 14 evidence-based regulatory choices to have public reasoning and democratic accountability and judicial review.

VII. CONSTITUTIONAL ACCOUNTABILITY, REGULATORY DESIGN, AND THE WAY FORWARD

A. The Precautionary Principle and Environmental Technological Risk

The regulations fail to address environmental impacts which arise from the initial stages of technology implementation. Data centres which operate at large scale use vast amounts of electrical power. The fast pace of product development leads to a situation where consumers discard more electronic devices than current recycling systems can handle. The environmental impacts of cryptocurrency mining operations create distinct measurable impacts on nature. These issues hold significant importance because existing laws already address them. The Supreme Court recognized the precautionary principle as a customary international law in Vellore Citizens Welfare Forum v Union of India[41] which empowers India through Article 51(c). The Supreme Court established the absolute responsibility standard for dangerous industries in MC Mehta v Union of India,[42] which serves as a legal framework that courts can utilize to assess the environmental effects of technology firms. The state and citizens must protect the environment according to Articles 48A and 51A(g) of the Constitution. This protection duty requires all citizens to observe this duty which includes safeguarding the environment from digital economy environmental impacts.

B. The Institutional Architecture of Technology Regulation

The regulatory gap mapping process shows an ongoing institutional problem. The existing regulatory bodies require new design standards because their current technological environment exceeds their original design capacity. The Data Protection Board created under the DPDPA functions primarily as a complaint's adjudicator rather than a proactive regulatory authority with standard-setting and surveillance functions. The CCI, for all its recent dynamism, operates

[40] *Shyam Telecom Ltd v BSNL* (2011) Delhi HC 1248.
[41] *Vellore Citizens Welfare Forum v Union of India* AIR 1996 SC 2715.
[42] *MC Mehta v Union of India* AIR 1987 SC 1086.

 [ISSN 2581-5369]

mainly through reactive ex post investigation. The Telecom Regulatory Authority of India, reconstituted under the Telecommunications Act 2023,[43] has expanded powers but remains oriented toward conventional telecommunications rather than the AI-enabled services increasingly delivered over telecom infrastructure. The Drone Rules 2021[44] address one particular technological deployment context but exemplify the sectoral fragmentation that characterises India's technology regulatory architecture more broadly.

Both the Law Commission's Report No 269 on Human DNA Profiling[45] and the Justice Srikrishna Committee's foundational report on data protection[46] recommended the creation of regulatory bodies that are specialised, technically competent, statutorily independent, and structured for genuine multi-stakeholder participation. The DPDPA has implemented some of these recommendations yet they require complete implementation through legislative processes. The NITI Aayog's AI strategy development work shows that emerging technology governance systems need to function as dynamic systems which evolve through time to meet changing needs.

C. Health Technology, Medical AI, and the Right to Life

The application of artificial intelligence in healthcare presents some of the most acute constitutional questions the regulatory gap generates. The Supreme Court's recognition in Paschim Banga Khet Mazdoor Samity v State of West Bengal[47] of a constitutional right to emergency medical care within the right to life under Article 21 has implications for how AI diagnostic tools should be deployed in public health settings. If an AI diagnostic system trained predominantly on data from populations that do not reflect India's demographic diversity systematically misdiagnoses conditions affecting particular groups, then its deployment in public hospitals may not be merely a clinical error but a constitutional harm.

The existing regulatory framework for medical technology the Indian Medical Council Act 1956[48] and the NITI Aayog telemedicine guidelines was designed for a world of human practitioners and provides no meaningful guidance on AI-assisted or AI-led diagnosis. The standard of professional negligence articulated in Poonam Verma v Ashwin Patel[49] requiring

[43] The Telecommunications Act 2023 (Act 44 of 2023).
[44] The Drone Rules 2021 (Ministry of Civil Aviation, Notification S.O. 3132(E)).
[45] Law Commission of India, Report No 269: Human DNA Profiling (2017).
[46] Justice BN Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and IT 2018).
[47] *Paschim Banga Khet Mazdoor Samity v State of West Bengal* AIR 1996 SC 2426.
[48] The Indian Medical Council Act 1956 (Act 102 of 1956).
[49] *Poonam Verma v Ashwin Patel* AIR 1996 SC 2111 (Supreme Court of India).

practitioners to adhere to established clinical protocols begs the question of what protocols should govern a clinical process in which the recommending entity is not a person but a model. Whether the liability for AI-generated clinical error rests on the developer, the deploying institution, or the supervising clinician is a question with immediate consequences for both civil liability and the criminal law of negligence under the BNS, and it awaits legislative resolution.

D. Towards a Principled Framework for Closing the Regulatory Gap

The research presented in this paper establishes five specific recommendations which stem from constitutional principles instead of theoretical policy preferences. Proportionality should establish itself as a mandatory worldwide benchmark which technology regulation must follow. All legislative or executive actions which use technology to implement or limit fundamental rights must comply with Puttaswamy's four-part proportionality assessment. Courts need to follow this standard with strict enforcement while dismissing all claims which state that technical matters or national security needs create exceptional situations through which their evidence requires less strict assessment.

All algorithmic accountability practices must receive establishment through constitutional law. People need to access the explanation for important automated decisions because this right arises from Article 14 protection against random decision-making and Article 21 safeguarding of their legal rights. Parliament must create legal rules which define this right through both DPDPA and a separate AI governance law. The EU AI Act's risk-based classification model[50] provides a useful comparison which needs adjustment to fit India's constitutional system and its development requirements.

Third, the electronic evidence framework needs to update its systems in accordance with modern AI technology which produces new content. The BSA has made real improvements which still do not meet all requirements. Statutes need to establish the authenticating process which determines how results should be handled in court after they undergo testing. The constitutional right to fair trial demands nothing less.

Fourth, competition regulation must evolve toward an ex-ante model for gatekeeper platforms. The Competition (Amendment) Act 2023 moves in this direction, but the definition of systemically significant digital enterprises and the presumptive obligations applicable to them require further legislative development. The CCI must be endowed with the technical expertise, information-gathering powers, and institutional resources necessary for real-time digital market

[50] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM(2021) 206 final.

 [ISSN 2581-5369]

monitoring.

Fifth, Parliament should enact a dedicated AI Governance Act, establishing a statutory AI Regulatory Authority with technical expertise requirements, sector-specific AI standards, mandatory impact assessment obligations for high-risk AI systems, and a public AI register. This recommendation is consistent with the NITI Aayog's own AI strategy document[51] and has been supported by Parliamentary Standing Committee reports.[52] It represents the most urgent legislative gap identified by this study.

VIII. CONCLUSION

The regulatory gap between emerging technologies and India's existing legal structures is real, wide, and constitutionally urgent. This paper has demonstrated through empirical doctrinal analysis that it manifests across four distinct dimensions — definitional inadequacy, institutional incapacity, remedial ineffectiveness, and constitutional accountability deficit — and that it pervades every major domain of legal ordering from criminal justice to competition policy, from data governance to public health.

There is, however, a degree of cautious optimism available. The Indian Constitution contains within its text and structure all the normative resources necessary to address the gap, provided there is willingness to deploy them. The legal framework emerges from four components which include Puttaswamy's proportionality review, Anuradha Bhasin's digital rights extension, the Pegasus ruling on privacy rights regarding surveillance tools, and Shreya Singhal's demand for constitutional evaluation of technology laws. The decisions establish a constitutional framework which defines the boundaries for constructing solutions to the regulatory issue.

The 2023 legislative developments which include the new criminal codes, the DPDPA, the Competition Amendment and the Telecommunications Act trying to represent a substantial effort to update India's regulatory framework. The system has reactive elements which respond to existing issues but it lacks complete coverage which should be provided through its comprehensiveness. The machine operates at a speed which exceeds all legal limits according to what this paper has established. The Constitution serves as an effective framework which enables institutions to fulfil their duties when they choose to take their responsibilities seriously.

The process of converting technological capabilities into legal responsibilities requires more than technical skills and administrative tasks. The project establishes a constitutional framework

[51] NITI Aayog, Discussion Paper on National Strategy for AI (Government of India 2018) 34.
[52] Standing Committee on Information Technology, Parliament of India, *Suspension of Telecom Services/Internet and Its Impact: 47th Report* (Lok Sabha Secretariat 2021).

 [ISSN 2581-5369]

which requires complete implementation. A society becomes unconstitutional because it allows algorithms to make decisions for its citizens while there exists no legal mechanism to control those decisions. The evidence presented in this paper demonstrates that effective preventive regulation now operates within a diminishing time frame. The existing legal system currently exists as established. The constitutional framework maintains its structural integrity. The necessary requirement involves both legislative and institutional determination.

*****

 [ISSN 2581-5369]

IX. BIBLIOGRAPHY

Cases

1. Anvar P.V. v P.K. Basheer (2014) 10 SCC 473 (Supreme Court of India).
2. Anuradha Bhasin v Union of India (2020) 3 SCC 637 (Supreme Court of India).
3. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (Supreme Court of India).
4. Competition Commission of India v Google LLC, Case No 7 of 2012 (Competition Commission of India 2022).
5. Competition Commission of India v Google LLC, Case No 39 of 2018 (Competition Commission of India 2022).
6. Foundation for Media Professionals v UT of Jammu & Kashmir (2020) 5 SCC 746 (Supreme Court of India).
7. In re: Pegasus Project (2022) 9 SCC 1 (Supreme Court of India).
8. Justice K.S. Puttaswamy v Union of India AIR 2017 SC 4161 (Supreme Court of India).
9. Justice K.S. Puttaswamy v Union of India (Aadhaar) (2019) 1 SCC 1 (Supreme Court of India).
10. Maneka Gandhi v Union of India AIR 1978 SC 597 (Supreme Court of India).
11. MC Mehta v Union of India AIR 1987 SC 1086 (Supreme Court of India).
12. Mukesh v State (NCT of Delhi) (2017) 6 SCC 1 (Supreme Court of India).
13. Paschim Banga Khet Mazdoor Samity v State of West Bengal AIR 1996 SC 2426 (Supreme Court of India).
14. Poonam Verma v Ashwin Patel AIR 1996 SC 2111 (Supreme Court of India).
15. Raj Gopal v State of Tamil Nadu AIR 1995 SC 264 (Supreme Court of India).
16. Ram Jethmalani v Union of India (2011) 8 SCC 1 (Supreme Court of India).
17. Ratan Tata v Union of India (2014) 8 SCC 410 (Supreme Court of India).
18. Satendra Kumar Antil v CBI (2022) 10 SCC 51 (Supreme Court of India).
19. Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801 (Supreme Court of India).
20. Shreya Singhal v Union of India AIR 2015 SC 1523 (Supreme Court of India).

 [ISSN 2581-5369]

21. State of Haryana v Bhajan Lal AIR 1992 SC 604 (Supreme Court of India).
22. Telefonaktiebolaget LM Ericsson v Competition Commission of India (2016) DELHC 2114 (Delhi High Court).
23. United States v Google LLC, No 1:20-cv-03010 (US District Court, District of Columbia 2023).
24. Vellore Citizens Welfare Forum v Union of India AIR 1996 SC 2715 (Supreme Court of India).
25. Vivek Narayan Sharma v Union of India (2023) 4 SCC 1 (Supreme Court of India).
26. Yashwant Sinha v CBI (2019) 6 SCC 1 (Supreme Court of India).

Legislation

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Act 18 of 2016).
2. Bharatiya Nagarik Suraksha Sanhita 2023 (Act 46 of 2023).
3. Bharatiya Nyaya Sanhita 2023 (Act 45 of 2023).
4. Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023).
5. Competition Act 2002 (Act 12 of 2003).
6. Competition (Amendment) Act 2023 (Act 18 of 2023).
7. Constitution of India 1950.
8. Digital Personal Data Protection Act 2023 (Act 22 of 2023).
9. Drone Rules 2021 (Ministry of Civil Aviation, Notification S.O. 3132(E)).
10. Indian Evidence Act 1872 (Act 1 of 1872).
11. Indian Medical Council Act 1956 (Act 102 of 1956).
12. Indian Penal Code 1860 (Act 45 of 1860).
13. Information Technology Act 2000 (Act 21 of 2000).
14. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
15. National Green Tribunal Act 2010 (Act 19 of 2010).
16. Telegraph Act 1885 (Act 13 of 1885).
17. Telecommunications Act 2023 (Act 44 of 2023).

 [ISSN 2581-5369]

18. European Parliament and Council Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
19. Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1.
20. European Commission, Proposal for a Regulation on Artificial Intelligence (AI Act) COM(2021) 206 final.

Books and Articles

1. Balkin J, 'The Three Laws of Robotics in the Age of Big Data' (2017) 78 Ohio State Law Journal 1217.
2. Calo R, 'Robotics and the Lessons of Cyberlaw' (2015) 103 California Law Review 513.
3. Lessig L, Code: And Other Laws of Cyberspace (Basic Books 1999).
4. Marchetti G, 'AI Regulation: A Practical Guide to Emerging Frameworks' (2022) 34 Harvard Journal of Law and Technology 189.
5. Pasquale F, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015).
6. Pasquale F, New Laws of Robotics: Defending Human Expertise in the Age of AI (Harvard University Press 2020).
7. Schwab K, The Fourth Industrial Revolution (World Economic Forum 2016).
8. Zuboff S, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Public Affairs 2019).

Government and Official Reports

1. Justice BN Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and IT 2018).
2. Law Commission of India, Report No 269: Human DNA Profiling (2017).
3. Ministry of Law and Justice, Report of the Committee on Reforms of Criminal Laws (Government of India 2020).
4. NITI Aayog, National Strategy for Artificial Intelligence: AI for All (Government of India 2018).
5. NITI Aayog, Telemedicine Practice Guidelines (Government of India 2020).
6. Standing Committee on Information Technology, Parliament of India, Suspension of Telecom Services/Internet and Its Impact: 47th Report (Lok Sabha Secretariat 2021).

 [ISSN 2581-5369]