Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The DPDPA 2023 and Beyond: Data Localisation, AI Regulation, and the Future of Privacy in India

Ambar Gupta[a]

[a]CHRIST (Deemed to be University) Delhi NCR, India

Received 20 May 2025; *Accepted* 21 June 2025; *Published* 25 June 2025

Digital Personal Data Protection Act (DPDPA) 2023 is a major undertaking within the legal framework in India as it provides rules and regulations that safeguard the privacy of personal information and at the same time tackles the issue in the realm of the information economy. It imposes heavy requirements on data stewards by integrating ideas like consent, data minimisation and the right to erase. However, there is still a barrier to obtaining, including government exemptions, data localisation, and poor enforcement channels, which question its efficiency. Besides information privacy, Artificial Intelligence-powered methods of surveillance, including biometrics, predictive policing, and facial recognition, transform the process of law enforcement, offering efficiency and threatening civil rights. The advancements demand urgent regulatory frameworks to resolve the security and moral problems. This analysis shows how DPDPA is implemented, the legal implications of AI surveillance, and the unclear policies covering social media to compare them with overseas regulations to highlight their flaws. DPDPA requires changes in the future: judicial control, new legislation on any emerging digital risks, and adherence to international standards. The interconnection of the notions of privacy and digital sovereignty with technological progress will affect the future of the data protection of India and demands further revisions to ensure effective privacy in the globalised digital world.

Keywords: *digital protection, cross-border data transfer, artificial intelligence, surveillance, data sovereignty.*

INTRODUCTION

In a world where technological progress takes a predominant part, the field of interaction between the law and digital innovations is an urgent topic of discussion. Digital Data Protection 2023[1] will be a historic addition to the legal system of India as it tries to balance the privacy of individuals and the challenges of a data-driven economy. The Act aims to even the balance by introducing the principles of consent, data minimisation, and the right to be forgotten, among others, and placing substantial requirements on data fiduciaries. Nevertheless, there are still some bumps on the way- governmental exemptions, data localisation requirements, and a lack of a solid enforcement structure make it questionable how effective it will be.

The Act is a paradigm change in this direction, codifying important values, like consent, data minimisation, limitations, and the right to be forgotten, giving individuals more control over their data. Nonetheless, the history of the DPDPA is full of acute contradictions. The government is providing broad exemptions to state surveillance and national security, which may hurt the principles on which it is founded. Moreover, the success of the Act is dependent on the very question of whether the enforcement mechanism, the Board of Digital Protection (DPBI), will be robust and independent, which remains to be seen, and creates the issue of institutional capacity and oversight gaps.

In addition to the fundamental provisions of the DPDPA, new technology such as Artificial Intelligence is drastically changing areas like surveillance and policing and is creating new ethical and legal dilemmas that current legislation finds difficult to handle. These tools are AI-enhanced facial recognition, biometric tracking, predictive policing algorithms, and automated risk assessment tools, all of which purport to offer increased efficiencies but run the very real risk of infringements of massive proportions on civil liberties. Such technologies are black-boxed, allowing pervasive surveillance of the population, reinforcing algorithmic discrimination, and possibly automating discrimination, and lack accountability models. The existing provisions of the DPDPA contain little advice on how to regulate such automated decision-making or reduce AI-specific harms, demonstrating a significant regulatory gap.

[1] Digital Data Protection 2023

What is immediately required is a subtle law that would protect the so-called chilling effect of mass surveillance and allow lawful uses of the surveillance by law enforcement.

At the same time, controlling social media networks is one of the troubled battlegrounds. Some of the positive effects of platforms include the magnification of discourse in society, whereas virulent hate speech, misinformation, and targeted harassment can spread. The Governments around the globe, including that of India, are pressing harder to get the platforms to be more responsible when it comes to the moderation of content. However, this requirement conflicts with other essential principles, freedom of speech and digital rights. Regulation is a challenging task to design: we cannot want to hold platforms liable only for systemic risks, without wanting to either over-censor or transfer necessary aspects of government functions to them through regulation.

Social media & Hate Speech: Assessment of the problems of policing online harm without limiting free speech and by the current concepts of digital rights. Through comparative research to global regimes such as the GDPR in the EU, this article presents the missing links and possible avenues towards enhancing India's digital governance regime. It holds that adequate regulation requires not only the presence of strong legislation, such as the DPDPA, but also the constant alignment with technological changes, strengthening of the regulatory authorities, and the resolute determination to reconcile conflicting fundamental rights in the digital era.

CONTEXT, REGULATORY FRAMEWORK & OTHER NOTABLE CONSIDERATIONS OF DATA LOCALISATION, ARTIFICIAL INTELLIGENCE AND FUTURE OF PRIVACY

The **Digital Personal Data Protection Act 2023** is a landmark Act that will protect the privacy of the people in the era of digital India. The Act is a culmination of a greater than five-year period of negotiations brought about by a landmark SC judgment in Justice K.S. Puttaswamy v The Union of India,[2] whereby it has been held that the right to privacy is a fundamental right under Article 21 of the Constitution of India[3]. The pressing need to have a legal framework to protect this right forced the government to release the different drafts over the years, beginning with the report of an expert committee in the year 2018, the Personal Data

[2] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1

[3] Constitution of India 1950, art 21

Protection Bill in 2019, a parliamentary debate in 2021, and finally, the amended version in 2022. Both versions presented the varying approaches to the matter of the equalisation of the rights of individuals and the needs of the state and the businesses to process data. India passed DPDPA as the first cross-sector data protection law on August 11, 2023. It will work towards the development of digital trust in the protection of personal information and legal data processing, which is a major step toward improving the Indian digital governance in the country.

PRECIOUS AND LEGAL DOCTRINES

The DPDPA sets a rights-based approach to individuals (the so-called Data Principals) and adds many responsibilities to the parties working with personal data (referred to as Data Fiduciaries) and their service providers (Data Processors). Important ideas that govern it are:

Consent: Consent in current data protection laws, including DPDPA in India, should be unconditional, clear, informed, and specific; it should be expressly demonstrated by a deliberate and voluntary process of the person. There is no possible enforcement or implication of it. Notably, it should allow people to cancel this authorisation easily, as was the case in the granting of the permission.[4]

Purpose Limitation: Personal data may not be used without being on a legal basis, causing no doubt about the purpose and shall be in full consent with the person, or otherwise falling under 12 defined purposes of using personal data established in the Act (state benefits, employment, etc).[5]

Storage Limitations: The data is not stored forever. Such retention must not be permitted beyond the extent and duration needed by the stated purpose unless the law requires it.[6]

Security Protocols: Data Fiduciaries should also apply adequate technical and organisational security measures to ensure that data breaches do not occur.[7]

[4] The Digital Personal Data Protection Act 2023, s 6

[5] The Digital Personal Data Protection Act 2023, s 5

[6] The Digital Personal Data Protection Act 2023, s 8

[7] The Digital Personal Data Protection Act 2023, s 8(5)

LAW, TECHNOLOGY & AI IN MONITORING

Facial recognition, predictive policing, and other AI-based surveillance are interesting privacy issues as their use increases. The Digital Personal Data Protection Act addresses these issues, but not in detail. Although it promotes such principles as consent, fairness and data minimisation, Section 17 permits broad derogations to state security and maintenance of public order with few protection mechanisms. Consequently, it creates the possibility of algorithmic bias, profiling, and abuse, the results of which are not transparent and accountable. However, unfortunately, there is still some control limited to such ancient laws as the Indian Telegraph Act 1885[8] and the CrPC 1973, which do not correspond to the present-day digital picture. The Pegasus spyware case and, in particular, the Puttaswamy case (with the need to apply a necessity and proportionality test) prove how necessary it is to implement stricter legal regulation of surveillance tools in India.

In the realm of hate speech conversation and online space, the idea is to strike a balance between the freedom of expression[9] and the necessity to respond to harmful dismissal. DPDPA concentrates on the collection and processing of user data by the platforms, whereas the IT Act[10] and the most recent IT Rules, 2021, regulate content moderation. Yet, the implementation appears to be irregular in many ways. Shreya Singhal v Union of India[11], ambiguous laws such as Section 66A[12] were abolished, but the means of effective and responsible moderation, along with the guarantee of user rights, remain doubtful.

KEY PROVISIONS

Non-Residents Applicability: The DPDP Act applies to people and corporations in India who collect the data of Indian residents. It is particularly notable that it also applies to non-citizens living in India, whose data processing takes place outside of India in terms of any activity that is related to the provision of goods or services. The example refers to the digital service/goods sent to an NRI citizen staying in India by a private party in another country.

[8] Indian Telegraph Act 1885

[9] Constitution of India 1950, art 19(1)(a)

[10] Information Technology Act 2000, s 79

[11] *Shreya Singhal v Union of India* (2015) 5 SCC 1

[12] Information Technology Act 2000, s 66A

Data Gathering and Data Handling Goals: The Bill of 2023 allows processing data on personal grounds on any legal basis. The user or owner of the data may die, but the organisation which manages the data may either seek permission from the individual concerned or may use it in what is known as 'Genuine Uses' as defined by the law. It is required that consent be made voluntary, precise, knowledgeable, unrestricted, and clear, with an explicit affirmative action towards a particular goal. The data obtained should be limited to only the necessary data for the targeted mission. This information should be provided in a transparent notice to the users to explain the rights of the concerned person and the complaint redressal procedure. People are allowed to withdraw the authorisation provided that the authorisation is the ground of the processing of data.

Legitimate Use Embodies the following:

(a) When an individual voluntarily presents personal information for a designated purpose;

(b) when any subsidy, benefit, service, license certificate or permit is provided by any agency or department of an Indian state, as long as the individual has previously consented to receive any other kind of similar service by the Indian state (this can raise some issues as it would enable all the Indian state agencies and departments providing such services to access any personal data held by other Indian state departments and agencies).

TENSIONS AND FUTURE CHALLENGES

Data Localisation Requirements Moderation: The 2023 law takes a U-turn on the problem of data localisation. Whereas the bill in 2019 limited some of the data flows, the 2023 law merely says that the government can restrict the flows to specific countries by giving a notification. Although this is not stated out, the authority to control data flow appears to be in order to grant the government the same legal powers that are also vital to national security. According to the law, this will also not affect actions of the sector-specific agencies which have or could impose localisation requirements. As an example, the localisation requirements of the Reserve Bank of India will remain legal.

AI Development v Rights Protection: Making sure that the balances that come with AI development (transparency, equity, reductions in bias) are not travelling at the expense of advancement. Government Exemptions: Magnitude and control of wide exemptions in national interest, social order, et cetera, still stand out as an urgent problem to privacy. Enforcement Capability: Increasing the ability of the DPBI to handle complex cases (which includes cases on AI) and take measures against large entities. Harmonisation Complexity: The facilitation of blending well into the current law and future sectoral laws.

MAIN ARGUMENT & CASE LAWS

The Digital Personal Data Protection Act (DPDPA) 2023, introduced in India, is the result of a constitutional evolution in a country where the concept of law is covered with a jungle of intricacies. We will complement the analysis of its basic arguments with some law details and human consequences:

The Constitutional Necessity: The Perennial Impact of Privacy –

Central Claim & Human Consequences: The DPDPA is more than a regulatory framework; it reflects the legal content of the fundamental right to privacy enshrined in Puttaswamy (2017). Before Puttaswamy, 'Privacy' was an ambiguous concept, which could easily be ignored. The 9-judge bench firmly affirmed: Privacy becomes a part of human dignity and independence according to Article 21. This serves to mean that every Indian citizen is entitled to a constitutional barrier against the unreasonable invasion of their personal lives, including their communications, relations, minds, and health. The DPDPA is the direct response to this directive on a legislative level, as it tries to regulate the handling of this sensitive information by organisations (mostly businesses) in the digital age.

State Exemptions: A Shrouded Pool of Authorities: Section 17 of the Digital Personal Data Protection (DPDP) Act[13] imposes blanket exceptions on the government on the grounds of unclear expressions like the security of the State and public order. However, these misleading phrases are worrying in terms of misuse in India, although in appearance, crucial. Imagine a reporter exposing a faction of corruption, a demonstrator protesting against an important government project, or someone belonging to a discriminated group - their data, including personal messages, localisations, and contact list, may be accessed without their consent or knowledge and without any legal action being possible. This creates a dangerous

[13] Digital Personal Data Protection Act 2023, s 17

environment of free speech and dissent and extremes the freedom guaranteed by the Constitution.

The 1997 PUCL decision made it clear that even when surveillance is based on national security, it is supposed to be within the scope of the regulations, i.e. there have to be documented orders and a review committee is to be kept in check. Section 17 of the DPDP Act, however, does nothing to give such safeguards or counterweights. There is no need for any prior permission, judicial scrutiny or independent checks.

The current events, like the Pegasus spyware scandal, are a testimony to the destructive nature of uncontrolled surveillance. Advanced technology in the military was allegedly used to infiltrate the phones of journalists, judges, as well as activists. Where Section 17 is also misused, then it may be used to carry out such acts secretly, and the victims would have no avenue to pursue assistance. Several nations deal with this in different ways. GDPR gives exceptions to the EU and focuses more on transparency and control. In the US, the surveillance schemes have to go through the Foreign Intelligence Surveillance Court. Such protections are unavailable in the legislation of India, so Section 17 poses a great threat to personal freedom.

THE DATA PROTECTION BOARD: INDEPENDENCE IS NON-NEGOTIABLE

Central Claim & Human Impact: A regulator perceived to be a lackey of the government cannot incite confidence in the population, nor have a hope of taking on powerful players (Be it Big Tech or the government itself). This is necessary because the people who provide information about a data breach performed by a large company or their opposition to state surveillance through Section 17 need to first know that the decisionmaker will be impartial and brave. Without this, the promises of the DPDPA become vain. Firms also need a uniform, impartial enforcement.

Enhancement of Judicial Procedures: Rojer Mathew v South Indian Bank Ltd (2019)[14] having ruled upon tribunal appointments, in general, the Supreme Court emphasised that tribunals performing crucial judicial functions should be safeguarded to ensure their neutrality against

[14] *Rojer Mathew v South Indian Bank Ltd.* (2020) 6 SCC 1

the Executive (particularly the appointment and removal process), which is in line with the concerns that are exuding in terms of the DPB.

In Madras Bar Association v Union of India (2020 & 2021),[15] the series of rulings struck down tribunal amendments. The Court ruled that tribunals should not be part of the ministry that sponsors them, and their composition must ensure independence and fairness.

The fact that its organisation (appointment of its members by the government; government-set rules dealing with crucial topics like cross-border data and exemptions) fails to fall under these criteria is evidenced through Ministry of Defence v Babita Puniya (2020).[16] Also pointed out that the independence of adjudicative bodies is a part of the basic fabric of the Constitution. These are some of the grounds through which a weak DPB is likely to be challenged on constitutional grounds.

DATA LOCALISATION: SECURE OR COST-CONSTRAINT?

Key Message & People Impact: The necessity to keep information in India can appear to be a chauvinist approach, but it costs much. Small and medium-sized enterprises and their startups that rely on cost-efficient international cloud solutions (e.g., AWS or Azure) may face significantly more significant costs and operational complexity. Major corporations around the globe can reconsider their investments, which will impact employment and innovativeness. Consumers are likely to lose access to international services or pay more. Meanwhile, the actual benefits of increased security are disputed - motivated attackers can penetrate servers almost every time, regardless of their location. Is this duty achieving what its declarative purpose is in direct proportion?

Legal Environment, Examination: Proportionality test of the Puttaswamy (Legitimate Aim, Suitability, Necessity/Least Restrictive Alternative, Balancing) is crucial. Localisation proponents have agreed that localisation requirements fail a test of Necessity - are less restrictive solutions (effective contractual protections, encryption standards, and effective DPB oversight of transboundary flows) sufficient? Earlier attempts, including the RBI

[15] *Madras Bar Association v Union of India* (2020) 6 SCC 157
[16] *Ministry of Defence v Babita Puniya* (2020) 7 SCC 469

instruction on the localisation of payment data, met trade objections and implementation challenges, and presented a face of economic friction that lacked clear security benefits.

In B.N. Krishna v Union of India (2017)[17], the Court sounded alarms that data security is violated, without trying directly to say that having the data domestically is not a solution either. Data protection is a key to security, but it is not limited to where the data is located.

NEW TECHNOLOGIES: THE REALITY IS ALREADY BEING CHASED BY THE LAW

Central Claim & Human Impacts: The DPDPA regulates data collection and usage, but given the digital transformation to inference, profiling, and automation of decision-making processes involving AI, this will likely be a rule that will be broken in the future. Consider refusal of a loan, failure to appear in a job interview or being flagged by law enforcement as a risk because of an ambiguous algorithm with perhaps biased inputs, the DPDPA offers few fixes. Similarly, the noxious combination of hate speech, misinformation and virality on social media platforms requires some high-level regulation, which is not addressed by DPDPA, which focuses on data management. The citizens are left to choose between the threat to privacy by overdoing data collection to moderate the content and actual violence incited by uncommissioned hate speech.

Judicial Growth and Deficiencies –

Surveillance AI: Facial recognition cases challenging the technology, like those in Delhi or Telangana. Make prominent use of Puttaswamy. Petitioners argue that the introduction of mass surveillance, in the case there is a clear law defining it, its purpose and establishing stringent measures against abuse of such power, violates the Puttaswamy test. The S.17[18] is likely to confer immunity on the activities of the government from the scrutiny of the Act.

NRM of Content and Freedom of Expression: Shreya Singhal (2015) remains the staple. And vacated Section 66A[19] (with fine/imprisonment of messages that are considered offensive (online) as vague, with the protection of free expression. It continued the intermediary liability protections[20], but rearranged the situation, which said that so long as they diligently

[17] *B.N. Srikrishna v Union of India* (2012) WP (C) No 494/2012
[18] Digital Personal Data Protection Act 2023, s 17
[19] Information Technology Act 2000, s 66A
[20] Information Technology Act 2000, s 79

adhere to court and government orders to take down content, intermediaries will retain the safe harbour protection. However, the IT Rules 2021 require the obligatory use of pro-active moderation, which contradicts Shreya Singhal. The Delhi Government v Facebook, a case of 2021, highlighted the differences between platform responsibility and freedom of speech during a crisis.

THE MONEY BILL MANOEUVRE: A QUESTION OF DEMOCRATIC LEGITIMACY

Main Argument and Society Impacts: Passing a law on fundamental rights, which affects all income earners, as a Money Bill, is detrimental to the proper democratic scrutiny that the law deserves. The revising chamber, made up of the Rajya Sabha, which was to reflect the states, was ignored. This undermines the process of law-making and the law itself. It is politically convenient rather than considering rights issues critically and taking into consideration complex rights issues.

Widening Duties of Judges: Justice K.S. Puttaswamy (Retd.) v Union of India (Aadhaar Ruling-2018): The most obvious one. Though upholding Aadhaar as a valid document, most of the members of the 5-judge bench pronounced with a sense of serious apprehension, the classification of the Aadhaar Act as a Money Bill. Dissent presented by Justice Chandrachud cited it to be against the Constitution. Importantly, the Court referred the question about the validity of the Aadhaar Act as a Money Bill to a bigger bench (7 judges).

This aspect remains unaddressed, and it casts a shadow on DPDPA implementation. South Indian Bank Ltd. (2019)[21] focuses on the tribunal reforms passed under the Money Bill, the Court re-emphasised the concerns with the use of this process to pass laws carrying significant non-fiscal implications to rights and justice delivery, as was the case with Aadhaar and applicable to DPDPA.

Comparative Jurisprudence: The DPDPA 2023 Indian law on privacy is unique and different in comparison to other countries of the world when it comes to data localisation. Unlike GDPR from the EU, which aims to achieve a free flow by either adequacy decision or protection, the DPDPA follows a prohibited-unless-permitted basis, only permitting transfer to those countries which the government considers as white listed. This will set a stricter bar

[21] *South Indian Bank Ltd. v Union of India* (2019) 6 SCC 1

than the GDPR and will avoid the Chinese PIPL model of almost mandatory localisation of broad data categories, offering flexibility under specific conditions. Comparatively, it reflects the concern given to providing what and after all to what degree the digital sovereignty almost to the degree of indifference of Russia or Indonesia instead of the piecemeal approach of the EU or the fragmented, sectorial approach of the US that finds a balanced between the concern of security and the demands of global business but the practical impact is dependent on the whitelist that is not publicly available.

As far as AI regulation is concerned, DPDPA is very different compared to the unambiguous, risk-based AI Act adopted in the EU. Instead, it regulates AI only indirectly through the overarching principles of data protection, as well as giving individuals rights regarding important uses of automated decision-making. It implements privacy laws as a form of control over AI systems, which was also done with GDPR principles, but unlike the AI Act, it lacks any ban on AI systems or high-risk systems, and compliance assessments. It is a sharp contrast to a mainly voluntary NIST framework approach in the US, but places India somewhere between the retouches of the EU and adaptability of the US, relying on future industry- and sector-specific codes and then the proposed Digital India Act to give a broader AI policy.

International standards show substantial inconsistencies in connection with the future of privacy under the DPDPA. Leaving aside its different standard of proving the necessity exception, unlike the more stringent GDPR, the Puttaswamy protections grant individuals rights that are roughly equivalent to those in the GDPR, although the vast range of government-related national security/public order exceptions matches those allowed by the PIPL in China, so there are concerns about compliance with the core Puttaswamy privacy protections.

CHALLENGES AND CRITIQUE

Information Localisation, Uncertainty, and Implications to the Economy: The conditional data transfer model of the Act is ambiguous, since there have been no countries formally listed in the whitelist yet. This creates an uncertainty of control, which is witnessed *in* ***WhatsApp LLC v Union of India (2021)***,[22] in which challenges were brought against the

[22] *WhatsApp LLC v Union of India* (2021) WP (C) No 3199/2021

localisation of payment data by the RBI, as violating the proportionality by the RBI, as per Puttaswamy. The industry fears that effective hard localisation of what is meant by data critical, which is not well defined in the Act, may interfere with operations and cause costs to rise, a lesson learnt with the Russian data mirroring law, which was supported by LinkedIn in LinkedIn v Roskomnadzor.[23] For establishing trade barriers, however, it condemned this.

Surveillance of Superfluous and Democratic Decay: There are wide exceptions to Sections 17(2) (c) and 18 that provide state access to sovereignty or the aspects of public order without necessity and proportionality tests, directly infringing the Puttaswamy tripartite privacy principle - legality, necessity, proportionality. This draws concern as indicated in K.S. Puttaswamy, where the extent to grant national security exemptions were granted was limited. The Act, in the absence of any judicial oversight as was the case on the Telegram encryption in the EU, is also at risk of becoming a means equivalent to the Pegasus stories legal proceeding cases.

Institutional Vulnerability: Executive influence in the appointments/resources is a violation of the Vineet Narain v Requirements of self-governing regulators in the Union of India (1997)[24]. The fines (maximum 250 Cr), unlike GDPR (4% global revenue), do not serve as a deterrent, and there is no right of action by the individual unless one happens to be a specialist organisation, thus undermining enforcement, as in California in the CCPA.

Consent and Age Gaps: The mandate of parental consent to all persons under 18 gives little consideration to the contextuality and autonomous nature of adolescents that was brought out in Puttaswamy and may result in exclusion (e.g., health services), observes a judgment of Justice for Rights Foundation v Union of India (2018)[25].[26]

[23] Sarah Rainsford, 'LinkedIn blocked by Russian authorities' *BBC News* (17 November 2016) <https://www.bbc.com/news/technology-38014501> accessed 12 May 2025

[24] *Vineet Narain v Union of India* (1998) 1 SCC 226

[25] *Justice for Rights Foundation v Union of India* (2018) SCC Online Del 11959

[26] Digital Personal Data Protection Act 2023, s 9

RECOMMENDATION & WAY FORWARD

Data Localisation and Transfers: The government must expeditiously announce explicit requirements to qualify nations to be whitelisted under Section 17, as well as specify in plain terms what comprises Critical Personal Data, based on the inclusivity in the plan, avoiding any unwanted, stringent localisation. To prevent trade isolation, cross-border frameworks (i.e. SCCs) should comply with international standards (e.g., GDPR adequacy), as in the case study of WhatsApp LLC v Union of India (2021)[27] on proportionality.

AI Oversight: New requirements to continue with regular evaluations of AI risk with high-risk AI (biometrics and healthcare) and strict bias-auditor requirements being placed in JR or industry-specific codes. Future Digital India Act must include some means of ethical AI (e.g. deepfakes) protections, and remedies for harm to non-personal data: the lack of these is a concern in AI legal cases.

Governmental Interventions: amend provisions 17(2)(c) and 18 to include interventions found to align with Puttaswamy, by inserting requirements of judicial warrant to access information, as well as a stricter necessity-proportionality test, and safeguarding via parliamentary oversight on exceptions. As an alternative, it is necessary to refer to K.S. Puttaswamy to prevent the growth of surveillance.

Empower Institutions: Ensuring that the Data Protection Board (DPB) have operational independence by having legal immunity to government interference in terms of staffing and funding, as in Vineet Narain v Union of India (1997).[28] Enforcement should be on a scale-like level (e.g. percentage of international revenue) and create a limited personal right to bring a lawsuit to enhance deterrence.

Flexibility Directed toward Rights: Replace universal consent of minors with age-based consent (e.g., 13-16 years old in case of low-risk processing), and make it a matter of balance between child safety and autonomy.

[27] *WhatsApp LLC v Union of* India (2021) WP (C) No 3199/2021

[28] *Vineet Narain v Union of India* (1998) 1 SCC 226

CONCLUSION

DPDPA 2023 will be a very important step by India towards a rights-based digital economy, and its effectiveness will rely on the resolution of the main tensions between innovation, state power, and privacy necessities. Though the Act outlines some critical concepts, such as consent, data minimisation, and algorithmic transparency (Section 12), its ambiguous nature jeopardises the constitutional ideal stated by Puttaswamy.

In contrast, the conditional data localisation framework lacks the rigidity of China, but it is not without problems in implementation. It is unclear whether the country belongs to a special group of favourable access to cross-border data flows (i.e. what the Indian government calls a white list) or what exactly is considered critical data that a company can be requested to move to local services (a.k.a. what the Indian government calls critical data). In the absence of that, companies report challenges to comply reliably, which risks the disintegration of the Union of India (2021). The reliance on loose data rules in the Act leads to the unregulated epidemic of algorithmic bias, deepfakes, and high-risk apps, an anomaly that is noted in the current case of the lawsuit against ChatGPT and contradicts the Puttaswamy promise of dignity and non-discrimination.

More importantly, the many exemptions of the Act (Sections 17(2)c), 18 threaten democratic accountability. Allowing state access without prior de novo judicial review and need-proportionality analysis (in opposition to the K.S. Puttaswamy case) directly opens to the Pegasus scandal, posing the risk of indulging in surveillance excesses. India).

The matters are further worsened by the institutional vulnerability: the influence of the executive on the Data Protection Board deprives the ideals of autonomy of Vineet Narain, and there is no deterrence worthy of GDPR. India stands at a turning point after the year 2023. Triumph requires:

Rights-based Regulation: Enact localisation whitelist/essential data via broad-based consultations; add the element of proportionality proposed by Puttaswamy in governmental exceptions. Empowered institutions: Safeguard the DPB against executive influence and enforce payment of fines in proportion/compensation in cases of individuals.