International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 23-03-2026, Accepted: 23-04-2026, Published: 08-05-2026
Volume 12, Issue 2, 2026, Page No. 251-257

Surveillance capitalism 2.0 in India: Assessing state and corporate overreach in the age Of Social media And AI under the DPDP Act, 2023

Tanu Priya[1], Dr. Trapti Varshney[2]
[1] Amity Law School Noida, Amity University Uttar Pradesh, India
[2] Assistant Professor of Law, Amity Law School Noida, Amity University Uttar Pradesh, India

Abstract
The social, economic, and political Indian context has experienced a digital transformation, where a complex and hybridised version of data exploitation has been created that this paper refers to as Surveillance Capitalism 2.0 a system where state surveillance desires and corporate data mining systems become not opposing forces, but enhancing each other through artificial intelligence and social media infrastructure. Surveillance Capitalism 2.0 in India, in contrast to its first-generation predecessor, a market-driven phenomenon of behavioural data commodification by technology corporations, is defined by the coming together of governmental power and platform capitalism, which generates an architecture of social control, which is both commercially profitable and politically consequential.

In the current paper, the dual overreach is critically viewed in the light of the Indian constitutional law and the recently established Digital Personal Data Protection Act, 2023 ('DPDP Act'). Starting with the constitutional underpinnings of the informational privacy as a fundamental right in the Supreme Court of India decision in Justice K.S. Puttaswamy (Retd.) v Union of India (2017) that identified informational privacy as an essential right under Article 21, the paper asks the question of whether the DPDP Act fulfills the constitutional promise of informational self-determination or whether it institutionalizes then. Specific emphasis is placed on Section 17 of the DPDP Act, which authorizes the Central Government to waive the compliance of state instrumentalities with the data protection requirements by simple executive notification without the need to deliberate in parliaments or be subject to judicial review, which makes the statute structurally susceptible to the same constitutional challenges that struck down Section 66A of the Information Technology Act, 2000 in Shre.

The paper also examines how surveillance as a chilling effect on freedoms as guaranteed by Articles 19(1)(a) and 19(1)(g), the discriminatory aspect of AI-based algorithmic systems of governance towards the guarantee of equality (Article 14) and the constitutional inadequacy of the current framework of interception as stipulated in the Indian Telegraph Act, 1885 and by. Although the Bharatiya Nyaya Sanhita, 2023 [14], with its reform of substantive criminal law, is depicted to be conspicuously silent on the digital surveillance infrastructure, in which its broadly-worded provisions against dissent and public order offences are operationalised.

Basing its argument on comparative analysis of the General Data Protection Regulation of the European Union, the Brazilian Lei Geral de Proteção de Dados, and the Investigatory Powers Act, 2016, the United Kingdom, and international human rights law, such as Article 17 of the International Covenant of Civil and Political Rights and the United Nations General Assembly Resolution 68/167, the paper elaborates. It suggests five structural reforms on this basis: legislative instead of executive authorisation of state data exemptions; a standalone Surveillance Authorisation and Oversight Act requiring judicial warrants to interception; structural reform of the Data Protection Board of India to make it genuinely independent; mandatory algorithmic impact assessment of AI systems making consequential decisions; and repeal of the traceability requirement of the IT Rules, 2021 as disproportion.

The paper has concluded that the DPDP Act, as an historically important law in India as the first comprehensive data protection law, is more of a part solution to the problem of Surveillance Capitalism 2.0 than a serious tool of data sovereignty. In the absence of the reforms suggested below, the Act can be considered a slippery slope towards exactly the kind of overreach that both state and corporate should be restrained in that the constitutional right to privacy requires to be limited.

Keywords: Surveillance capitalism, DPDP Act 2023, right to privacy, informational self-determination, algorithmic governance, section 17 exemption, data protection board, puttaswamy, bharatiya nyaya sanhita, digital rights, India, OSCOLA

Introduction

Artificial intelligence and social media have brought a new paradigm of power that does not lie in the legislatures, armies, or corporations in the classical meaning of these terms but in data. Personal information has become a commodity, and is now no longer a marginal issue of technologists, but a main jurisprudential question of democratic law across the globe. India with over 900 million internet users and one of the quickest expanding digital economies in the world, is at an especially acute point of inflection. The intersection of violent state surveillance platforms, overactive corporate information mining and a new legislative environment in the shape of the Digital Personal Data Protection Act, 2023 ('DPDP Act') has led to a new legal environment that is at once both encouraging and risky.

Surveillance Capitalism is a term, coined by Shoshana Zuboff, to explain how the commodification of human behavioural data has become a raw material to predict and alter behaviour, as extracted and left without any meaningful consent, and commoditized at scale. Firstly, this phenomenon was mostly corporate in nature: websites such as Meta, Google, and Amazon had been collecting data to display targeted advertisements. In India, now, we see what

this paper calls the 2.0 version of Surveillance Capitalism the fully developed, hybridised model whereby state and corporate actors do not oppose each other, but rather exist in complementary, and even symbiotic, ways.Corporate data pipelines are used by the state to provide security and governance, and corporations are given regulatory forbearance and access to the market.

A critical look at this hybrid surveillance architecture in the context of Indian constitutional guarantees and statutory law is presented in this paper. It examines the DPDP Act, 2023 as a reaction to this two-fold threat, questions its normative gaps, and suggests a normative theory of authentic data sovereignty. The paper is divided into five sections Part II gives an account of the conceptual development of surveillance capitalism in India context; Part III discusses the constitutional aspect of the surveillance era, Part IV critically reviews the regulatory framework of the DPDP Act, Part V discusses judicial, legislative and civil society responses, and Part VI provides concluding remarks and reforms.

Surveillance Capitalism 2.0: Conceptual Framework And Indian Manifestations

1. Beyond Zuboff: The State-Corporate Nexus

The thesis on which Zuboff bases his argument places surveillance capitalism in the logic of accumulation behavioural data as surplus that is obtained out of the consumers who are at once the consumer as well as the raw material of the production process. Nevertheless, this framework which is mostly developed in the context of the Western liberal democracy demands a significant modification in the Indian political economy. The third dimension of the Indian experience is the emergence of a developing state with authoritarian inclinations that sees data not only as an economic resource, but as a strategic tool of government, social management and political legitimacy.

Surveillance Capitalism 2.0 architecture in India has three mutually-reinforcing foundations. To begin with, there is the stratum of corporate data grabbing, whereby social media platforms, fin-tech firms, health-tech establishments and e-commerce giants are collecting granular behavioral data on Indian users in ever-increasing quantities; This data is collected on the basis of the terms of service which are typically tough to read and legally one-sided. Second, there is that of the state surveillance regime, which encompasses legal devices like the Telegraph Act of 1885, Information Technology Act of 2000 (the 'IT Act') and government orders made under the IT (Procedures and Safeguards of Interception, Monitoring and Decryption) Rules, 2009; These orders give the government the right to access, intercept and utilize this data. Third, and this is the new aspect of version 2.0: it includes an algorithmic governance layer, where systems driven by AI, trained on social media data, will be deployed to predictive policing, dissent mapping and citizen scoring, and the boundary between commercial intelligence and state power will become blurred.

2. Indian Case Studies in Hybrid Surveillance

The history of Indian surveillance capitalism can be followed by means of various tangible developments. The Aadhaar biometric system, without the partial reading-down of the Supreme Court in Justice K.S. Puttaswamy (Retd.) v Union of India (Puttaswamy II), remains a national identification basal, which allows access by the state and authentication by the private sector. Its compulsory association with SIM cards, bank accounts and government welfare programmes have produced a centralised architecture of data never seen before.

The acquisition of Pegasus spyware by an Indian government agency that was discovered during the Pegasus Project investigation showed that the state was not averse to contracting commercial sellers of offensive surveillance equipment and quite literally outsourced its surveillance to a third party. The report of the Technical Committee of the Supreme Court on Pegasus, which despite the non-cooperation of the Union government was inconclusive, is a salient indication of how corporate instruments are turned into an instrument of state overreach.

Moreover, in 2018, the proposal of the Social Media Communication Hub (SMCH) was proposed, which was later appealed to the Supreme Court in the case of Antony Clement Rubin v Union of India. intended to consolidate social media data to be monitored by the government. The plan did not go through, but its conceptualization demonstrates the institutional desire to have social surveillance based on data. In more recent times, the instructions of the Ministry of Electronics and Information Technology (MeitY) in the form of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which prescribe traceability of encrypted communications is another structural push towards de facto delegation of platform privacy to state controls.

Constitutional Foundations: Privacy, Dignity And Informational Self-Determination

1. The Puttaswamy Architecture

Any criticism of surveillance capitalism in India has its constitutional foundation with the nine judge bench ruling in Justice K.S. Puttaswamy (Retd.) v Union of India (Puttaswamy I). The Court was unanimous that privacy is a basic right in Article 21 of the Constitution of India, and another intrinsic right of right to life and personal liberty. Perhaps the most broadly reasoning concurrence of Justice D.Y. Chandrachud was that informational privacy as a separate strand, which asserts that people should be allowed to regulate data produced by and about them.

This constitutional ruling has far-reaching consequences on surveillance capitalism. When the informational self-determination is a right, then the state and corporate actors collecting data without a true informed consent are committing action that is constitutionally impermissible. The proportionality criterion stated in Puttaswamy I, which was based on the triple-test in Modern Dental College v State of Madhya Pradesh. Stricto sensu, legality, legitimate aim and proportionality is the constitutional yardstick that must be applied to any surveillance regime.

2. Article 19 and the Chilling Effect of Surveillance

Article 21 is not the only one implicated in surveillance capitalism. It is significantly and under-theorised and connected to the freedom of expression that is guaranteed by Article 19(1)(a). The inevitable result of a chilling effect on free expression is where citizens are aware or have reasonable suspicion that their social media communications are being monitored by state agencies or even the platforms as the so-called deputised surveillance intermediaries. In Zakharov v Russia, the European Court of Human rights.

appreciated that the threat of mass surveillance, without prior warning, would put a chill on expression. This doctrinal position has not been wholly imported to Indian courts yet but the rationale is available in the constitution.
The traceability requirement of messaging services, such as WhatsApp, under the IT Rules, 2021, is especially a problem in this respect. The Rules, which force platforms to intercept end-to-end encryption to determine the first originator of messages, act as a national wiretap architecture that targets in particular encrypted speech speech which individuals had decided to encrypt specifically because of its sensitive nature. This directly relates to Articles 19(1)(a) and 19(1)(g), and its constitutionality is still awaiting its hearing in Madras High Court.

3. Article 14 and Discriminatory Algorithmic Governance

Another aspect of surveillance capitalism that is yet to be extensively discussed about the Indian constitutional jurisprudence is how it intersects the right to equality under Article 14. Artificial intelligence systems that have been trained with biased information about the past criminal history, credit history, social media behavior reproduce and exacerbate the existing disparities.s. In the case of predictive policing using such systems, credit scoring using such systems, or the allocation of welfare (such as the case of Direct Benefit Transfer systems), they constitute algorithmic discrimination.
In the case of the Uttar Pradesh Police, which is reported in investigative reports, the Predictive Policing System relies on the information available in social media and criminal history to create risk scores of individuals. This type of system, running outside of the law, judicial control, or even open methodology, may contravene Article 14 since it exposes individuals to negative outcomes based on opaque, unprovable algorithmic findings. It also brings the spectre of automated discrimination of marginalised communities, as it is already overrepresented in criminal databases.

The Dpdp Act, 2023: Architecture, Promise And Pathology

1. Legislative Genesis and Structural Overview

The Digital Personal Data Protection Act, 2023 ('DPDP Act') was the result of a long and contentious legislative process that had seen three previous versions of a data protection bill in 2018, 2019, and 2021 end up in the garbage after failing to pass through parliament.The DPDP Act is the first time that India has passed a comprehensive data protection law and the fact that it has finally come is constitutionally and commercially important.
The Act implements an environment around the idea of Data Principal (who personal data is about) and Data Fiduciary (who decides how and why to process personal data). It requires that personal information may only be used to the extent that it is lawful, with consent or on certain basis of justifiable uses. It creates a Data Protection Board of India ('DPBI') as the adjudicatory authority, imposes personal fines of up to ₹250 crore on individual violations and up to 550 crore on systemic violations of children data, and Data Principals rights of access, correction, erasure and grievance redressal.
The architecture of the Act conceptually inspired the European Union General Data Protection Regulation (GDPR), but deviates to it in non-neutral ways they are structurally consequential, especially when regarding the case of state overreach.

2. The Consent Architecture: Apparent and Real

The consent framework of the DPDP Act seems to be sound on the surface: Section 6 states that the consent should be free, specific, informed, unconditional and unambiguous with clear affirmative action. The Data Fiduciaries should give a notice in simple language specifying the personal data to be collected and the purpose of processing.
This framework however is greatly compromised by Section 7, which lists out legitimate uses grounds of processing that do not necessitate consent in any way. These are the performance of a function under the law or to the delivery of a service ordered by the Data Principal, processing under compliance with court orders and broadly processing by the State subsidies, benefits, services, certificates, licences or permits. The latter ground is practically unlimited in nature. Since the Indian state offers services, in practically every sphere of life, including ration cards and land records as well as health care, the consent rule can be entirely devoured by the exemption of the state services.
This is the same logic of surveillance capitalism that it claims to limit enshrined in a data protection statute. When state actors are free to process personal data to render any sort of service without permission, and the data is subsequently at risk of being leaked to law enforcement or intelligence services, the Act would then be an accomplice in the surveillance system, instead of a limitation on it.

3. The State Exemption Clause: Section 17 and its Constitutional Infirmities

Section 17 is the structurally most important part of the DPDP Act, and the part that is most directly applicable to the criticism of state-side surveillance capitalism. This is to allow the Central Government by notification to waive the obligations of the Act upon any instrumentality of the state on the basis of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or deterrence of incitement to commit cognisable offences.
This amounts to a blank cheque in the constitution. The exemption is not debatable by parliament of the particular notifications, no judicial review is necessary, and the terms are drafted in constitutional terms (sovereignty, public order) general enough to cover literally any intelligence or surveillance operation. No proportionality assessment is required, no mandatory review mechanism is necessary and there is no sunset clause.
This provision is very questionable in terms of its constitutionality. In Puttaswamy I, the Supreme Court considered that any violation of the right to privacy should meet the triple test of legality, a legitimate purpose and a proportionality test. An exception of undefined state instrumentalities, to vaguely defined ends, passes neither the specificity element of the test of legality nor the proportionality test. This is structurally similar to Section 66A of the IT Act which was put down by the Supreme Court in Shreya Singhal v Union of India is vague and exceeds its constitutional bounds..
Besides, Section 17 brings an imbalance which is directly prohibited by GDPR. Article 23 of the GDPR does allow member states to limit the data protection requirements but these limits must be a legislative measure[s] and must not

undermine the nature of the fundamental rights and freedoms. The Indian provision, however, places the decision to do so wholly on the executive, avoiding both the deliberation of parliament, and the judicial review, at the same time.

4. The Data Protection Board: Independence and Efficacy

The DPDP Act establishes Data Protection Board of India as a tribunal organization that is entitled to penalize, give directions, and listen to complaints. Nonetheless, the structure of the Board begs the question of independence. The Central Government appoints the Chairperson and the members based on the recommendation of a committee that is mainly constituted of government officials the Cabinet Secretary, the Secretary of MeitY and nominated experts. The primary composition does not include any judicial member, and civil society or academia does not have any mandatory representation.

Compare with the set up of the Information Commissioner in the United Kingdom which is a non-departmental public body with a commissioner who is appointed after a public process and is answerable to Parliament, or the Data Protection Commission in Ireland, which is statutorily independent and is answerable to the Oireachtas. The DPBI, however, is structurally inferior to the very ministry it is supposed to control, as the digital economy policy, as well as the composition of the board, is controlled by MeitY. This poses a conflict of interest that might undermine the capacity of the Board to take action against government entities.

5. Children's Data and the Platform Economy

The DPDP Act in Section 9, prohibits processing of personal data of children (under age 18) without any verifiable parental consent, and does forbid behavioural tracking, targeted advertising, and profiling of children altogether. It is among the strengths of the Act and follows the best practices of the world including the Age Appropriate Design Code in the UK.

Its adoption is however confronted with the problem of verification in a country where age records are not uniform and where the platforms are not provided with age verification mechanisms that are reliable and do not in themselves generate privacy hazards. Also, the Act does not specify what is meant by verifiable parental consent, and this is a crucial question that subsidiary rules, which are yet to be completed, address. The difference between the legal protection of the internet and the actual digital survival is enormous with India boasting about 430 million child internet users the highest number in the world.

Judicial, Legislative and Civil Society Responses

1. Judicial Responses: Expanding but Insufficient

The jurisprudence of surveillance and data protection has been approached by Indian courts in a number of landmark cases, but the jurisprudence is still somewhat scattered and in its infancy compared to the extent of the issue.

Puttaswamy I, is the most significant judicial action. the implication of which regarding surveillance capitalism remains to be played out in further litigation. In Puttaswamy II (the Aadhaar case), the Supreme Court supported the Aadhaar Act with changes, but placed substantial restrictions on its compulsory use by non-state actors a partial but substantial limitation on data fusion between corporations and the state.. The most advanced judicial expression of informational self-determination in India is the dissent given by Justice Chandrachud in Puttaswamy II, which would privation strike down the entire Aadhaar Act due to the possibility of surveillance and disproportionality.

In Virendra Khanna v State of Karnataka, the Karnataka High Court took into consideration the issue of whether it was possible to force WhatsApp metadata to investigate a crime, bringing up the speculation of privacy, surveillance, and electronic evidence. The Court determined that metadata, although not content, may have important privacy consequences and an important, although preliminary, step towards appreciating the privacy value of behavioural data.

The most forward-looking judicial platform to the issues of digital rights has become the Madras High Court. In S. Santhakumar v State of Tamil Nadu it discussed the social media surveillance by police and highlighted that surveillance of posts on social media based on political content without legal authorization infringes on the privacy and freedom of expression. Union of India v WhatsApp LLC. the Court is considering the constitutionality of the traceability requirement, which will probably become the next major case in digital rights after Puttaswamy I.

2. Legislative Gaps and Proposed Reforms

The DPDP Act, although it is a good initial step, also fails to address several crucial areas. Most importantly, India does not have a specific surveillance legislation. The constitutional foundation of the interception by the state is based on Section 5(2) of Indian Telegraph Act, 1885. a clause in colonial times that facilitated telegraphic communications and on Section 69 of the IT Act, authorizing interception in the name of sovereignty and integrity of India,

security of the State, or public order.. Nor was either of these provisions intended to be used in the era of AI-powered social media monitoring, or is either provision offered the judicial authorisation, proportionality considerations, or transparency conditions, which the new constitutional norms would require.

India does not, most importantly, have a wiretapping court that is similar to the Foreign Intelligence Surveillance Court (FISC) in the United States. or the statutory oversight committees set up by the Investigatory Powers Act, 2016 in the United Kingdom. Interception in India is legitimised on an executive level and can only be reviewed by a committee of top-ranking bureaucrats a quintessential example of the executive checking on its own.. The DPDP Act does not fix this structural deficit; it needs a separate Surveillance Reform Act that will ensure that interception is authorised judicially and that its proportionality is set, that it includes that mandatory notification is provided (at least after the surveillance) and that it contains independent parliamentary oversight.

In 2023, the Bharatiya Nyaya Sanhita (BNS), the new replacement of the Indian Penal Code, 1860, made alterations to the law on sedition and provisions on organised crime, but did not intervene with the digital surveillance infrastructure. The fact that the offences that are still open under the broadly-worded offence like Section 152 of the BNS (acts endangering sovereignty or unity) still stand creates the spaces where surveillance information obtained through the social media platforms can be used to

prosecute a crime on criminals dissent a trend that has been reported in the incidents involving activists, journalists and students convicted under the Section..

3. Civil Society, Activism and Digital Resistance

The ecosystem of civil society in India has reacted to the concept of surveillance capitalism more and more sophisticately, albeit with structural limitations such as the limitations to international civil society funding imposed by the Foreign Contribution (Regulation) Act, 2010 [16] which have limited the ability of organisations to operate.

The platform has been the most prolific litigant and policy advocate by the Internet Freedom Foundation ('IFF'), which has launched interventions in the cases including the challenge to the IT Rules, 2021 and the Pegasus petition. The Centre for Internet and Society has created the research groundwork on surveillance and data rights. Scholars like Amba Kak, Usha Ramanathan and Anushka Jain have created a normative structure in which the data protection discourses take place.

The application of end-to-end encrypted tools of communication, virtual private networks, and decentralised platforms has also become very rampant among activists, journalists and common users who want to avoid surveillance. Nonetheless, the traceability requirement contained in the IT Rules, 2021, in case enforced, may entirely harm the technical infrastructure of encrypted resistance.

Towards A Framework For Genuine Data Sovereignty

1. Data Sovereignty as a Constitutional Imperative

The normative concept that needs to inform the Indian reaction to Surveillance Capitalism 2.0 is the concept of authentic data sovereignty a concept that transcends consumer-rights model inherent in the DPDP Act and a concept of informational self-determination as a constituent of constitutional personhood.. This understanding of data sovereignty indicates that not just that individuals are able to access or modify their data, but that they have an inalienable right to manage the generation, processing and utilization of data that forms a digital representation of their self-identity.

This idea is based on three strands of the Constitution. The former is the ensuring of individual liberty and dignity by Article 21, interpreted through the Puttaswamy I prism. The second one is the Directive Principle in Article 39(b) that requires material resources of the community to be distributed to the common good an argument can be given that since data is a national resource produced by its citizens, it should be managed and not exploited to make money.. The third one is the new constitutional principle of democratic accountability which implies that the power of states should be open, argumentative and liable to external checks.

2. Reform Proposals

First, the Section 17 exemption of the DPDP Act must be significantly revised so as to provide that state exceptions to data protection must only be granted (not notified by executive) under parliamentary legislation, must be subject to a mandatory judicial review on challenge, must be time-limited, and must include a proportionality test.

Second, India needs a separate Surveillance Authorisation and Oversight Act, which mandates a judicial warrant to conduct any type of targeted and mass surveillance, which bans the use of AI-generated risk scores as the sole grounds to take action; it demands post-surveillance notification (even when delayed due to operational security reasons), and it establishes a parliamentary oversight committee, accessible to classified surveillance data.

Third, Data Protection Board should be redesigned in a more serious way to be truly independent. This entails that the Chairperson should have security of tenure (they can only be removed by a court process), it should have civil society, academic and legal profession representation on the Board, accountable to Parliament and not to MeitY and a statutory fund as opposed to government grants.

Fourth, The consequential decision-making processes of an AI system operated by a state or corporate actor based on scoring, welfare distribution, predictive policing, content moderation are required to undergo compulsory algorithmic impact evaluations, which must be publicly displayed in a registry, and cannot be individually challenged. The Right to Explanation, implicit in the due process aspect of Article 21, should be realised once again by supplementary provisions in the DPDP Act, or by specific legislation regulating algorithmic accountability.

Fifth, the traceability requirement pursuant to the IT Rules, 2021 should either be abrogated or reviewed by the constitution. The mandate that platforms decrypt end-to-end encryption is disproportionate, technically counterproductive (it will weaken the security of all users, including those in law enforcement) and constitutionally inappropriate under the Puttaswamy proportionality rubric.

3. The Role of International Law and Comparative Standards

India is a signatory and non-ratifying party to the International Covenant on Civil and Political Rights, but is a party to the ICCPR itself, which under Article 17 safeguards against arbitrary intrusion upon privacy. The UN General Assembly Speeches of 68/167 of the Right to to Privacy in the Digital Age upheld that the rights of people offline should be safeguarded over the internet. The adoption of DPDP Act and reforms of surveillance law in India need to be evaluated in comparison with these international commitments.

In comparison, the Brazilian Lei Geral de Proteção de Dados (LGPD). is a helpful template of an economy at the same level of development: it has stronger coverage of the state sector, more autonomous supervision, and a constitutional basis in Brazil, in Article 5, LXXIX, Article 5 that expressly proclaims the right to data protection as a fundamental right An amendment to the Constitution to explicitly inscribe the concept of data protection in the Indian Constitution on top of the unspoken Puttaswamy assurance would offer a more sustainable basis of data sovereignty.

Conclusion

Surveillance Capitalism 2.0 in India is not a threat 2.0 in the future but it is a current constitutional reality. The miring of state surveillance ambitions and corporate data collection infrastructures, which are facilitated by AI and social media platforms, has created a kind of power that cannot be identified in existing legal groups and is not limited by existing legal tools.

The DPDP Act, 2023, though having historical significance is more of a partial solution than a holistic solution. It has

compromised its consent framework with blanket legitimate-use exceptions; duplicates its own constitutional conflagration of error with its own state exemption clause; has no structural independence on its supervisory body; and is silent on the most consequential aspects of its own problem of digital power: algorithmic accountability, reform of the surveillance law, and encryption protection.

Puttaswamy I left constitutional foundations that are fruitful and fruitful. Constitutional values demand institute construction to be made alive. India does not just require a data protection law but a data sovereignty framework one that places the cause of informational self-determination as a constitutional right, creates independent control of the regulatory framework, acts algorithmic power is accountable, and imposes restraints on the appetite of the surveillance state by requiring it to be authorised by courts.

The ramifications of privacy are not confined to personal space. Unchecked, Surveillance Capitalism 2.0 will redefine the structural terms of democratic engagement in an ability to chill expression, selective prosecution, and create a self-censored citizenry aware of being surveilled at all times and places. Individual dignity, democratic governance and the rule of law contained in the Indian Constitution cannot co-exist with the surveillance-state constructed on the raw content of its citizens on-line lives. The law has to get on par and it has to do so with true autonomy, with structural acumen and constitutional boldness.

Bibliography

Primary Sources

Legislation

- Bharatiya Nyaya Sanhita 2023 [14]
- Digital Personal Data Protection Act 2023
- Foreign Contribution (Regulation) Act 2010 [16]
- Indian Telegraph Act 1885
- Information Technology Act 2000 [11]
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021[9]
- IT (Procedure and Safeguards for Interception, Monitoring and Decryption) Rules 2009
- Lei Geral de Proteção de Dados Pessoais (Brazil) Lei No 13.709/2018 [19]
- Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L119/1 (GDPR)

Cases

- Antony Clement Rubin v Union of India Writ Petition (Civil) No 1076 of 2019 [8] (Supreme Court of India)
- Justice K.S. Puttaswamy (Retd.) v Union of India (2017) [10] 10 SCC 1
- Justice K.S. Puttaswamy (Retd.) v Union of India (2018) 1 SCC 809 [5]
- Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353
- Roman Zakharov v Russia App No 47143/06 (ECtHR, 4 December 2015)
- S Santhakumar v State of Tamil Nadu (2022) SCC OnLine Mad 1823
- Shreya Singhal v Union of India (2015) 5 SCC 1
- Virendra Khanna v State of Karnataka (2021) SCC OnLine Kar 9426
- WhatsApp LLC v Union of India WP No 6272 of 2021 (Madras High Court)

International Instruments

- International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171
- UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167

Secondary Sources

Books

- Zuboff S, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019) [2]

Journal Articles

- Stone G, 'Free Speech in the Twenty-First Century: Ten Lessons from the Twentieth Century' (2009) 36 Pepperdine Law Review 273

Reports and Official Documents

- Amnesty International, India: Detained for Tweets (AI 2022) [15]
- Centre for Internet and Society, 'Surveillance Law in India' (CIS 2019)
- Information Commissioner's Office, Age Appropriate Design Code (ICO 2021) [9]
- Telecom Regulatory Authority of India, Annual Report 2022–23 (TRAI 2023) [1]
- UNICEF, The State of the World's Children 2023 (UNICEF 2023)

News and Investigative Reports

- Forbidden Stories and Amnesty International, 'Pegasus Project' (2021) [6] https://forbiddenstories.org/pegasus-the-new-leak/ accessed 10 April 2025
- Mohan A, 'UP Police's AI Surveillance Network' The Wire (New Delhi, 7 March 2023)

Refernces

1. Telecom Regulatory Authority of India. 'Annual Report 2022–23' (TRAI 2023), 2023, 14.
2. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019), 2019, 8.
3. Zuboff. (n 2) 93–94.
4. IT (Procedure and Safeguards for Interception, Monitoring and Decryption) Rules, 2009, 4.
5. Justice K.S. Puttaswamy (Retd.) v Union of India (2018) 1 SCC 809 ('Puttaswamy II'), 2018, 809.
6. Forbidden Stories, Amnesty International. 'Pegasus Project' (2021) https://forbiddenstories.org/pegasus-the-new-leak/ accessed 10 April 2025, 2021.
7. Justice K.S. Puttaswamy (Retd.) v Union of India (Pegasus) Writ Petition (Civil) No 314 of 2021 (Supreme Court of India, 27 October 2021) (Technical Committee Report, 2022), 2022.
8. Antony Clement Rubin v Union of India Writ Petition (Civil) No 1076 of 2019 (Supreme Court of India), 2019.
9. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 4(2).
10. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 ('Puttaswamy I'), 2017, 1.
11. Information Technology, 2000, 69.

12. Foreign Intelligence Surveillance Act of (USA), 50 USC Section 1803, 1978.
13. IT (Procedure and Safeguards for Interception) Rules, 2009, 16(4).
14. Bharatiya Nyaya Sanhita, 2023, 152.
15. Amnesty International. India: Detained for Tweets, 2022, 7.
16. Foreign Contribution (Regulation) Act, 2010.
17. International Covenant on Civil and Political Rights (adopted 16 December, entered into force 23 March 1976) 999 UNTS 171, art,1966:17:171.
18. UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167, 2013.
19. Lei Geral de Proteção de Dados Pessoais (Brazil) Lei No 13.709/, 2018.
20. Constituição Federal do Brasil 1988, art 5, LXXIX (as amended by Emenda Constitucional No of 2022), 1988, 115.