DATA AND THE STATE: A CONSTITUTIONAL INQUIRY INTO INDIA'S EMERGING DIGITAL GOVERNANCE FRAMEWORK

K. Sowmya, LLB (Hons.), School of Excellence in Law, The Tamilnadu Dr. Ambedkar Law University, Chennai

ABSTRACT

The rapid expansion of digital governance in India has brought the relationship between data, power and constitutional rights into sharper focus than ever before. While digital systems such as Aadhaar-linked welfare delivery, digital public infrastructure and large-scale data repositories promise administrative efficiency, they also create new sites of tension between the State's regulatory authority and the individual's right to privacy, autonomy and dignity. The constitutional framework, particularly after Justice K.S. Puttaswamy v. Union of India, recognises privacy as an intrinsic facet of Article 21. Yet subsequent developments reveal that the balance to be struck remains fragile. Legislations such as the Digital Personal Data Protection Act, 2023 and sector-specific regulations increasingly vest wide discretionary powers in the executive, often with limited judicial or parliamentary oversight.

This paper examines how India's emerging digital governance architecture has altered the scale and nature of State power. Drawing on key judgments, the study traces a judicial trajectory that oscillates between rights-based protection and administrative necessity. These legal developments are juxtaposed with the broader concerns of surveillance, profiling and behavioural regulation that accompany contemporary data regimes.

The paper engages with the dystopian imagination of George Orwell's 1984 as a conceptual lens through which unchecked data concentration and opaque State decision-making can be critically scrutinised. The comparison underscores how digital tools, if left unregulated, enable forms of observation and control, previously unimaginable in traditional governance structures. Ultimately, the paper reflects on how our core constitutional values should shape the way digital governance grows, stressing that even as the State's digital reach widens, the system must continue to protect individual freedoms and remain fair, transparent and accountable.

Keywords: digital governance, data privacy, surveillance, rights, orwellian

Digital Governance and the Quiet Rise of Big Brother

The rapid expansion of digital governance has fundamentally altered how the India exercises power and how individuals experience it. From Aadhaar-linked welfare delivery and digital public infrastructure to large-scale data repositories and algorithmic decision-making systems, governance today is increasingly mediated through data[1]. These systems promise administrative efficiency, inclusion and rationalisation of public services. At the same time, they reshape the constitutional relationship between the State and the individual by concentrating unprecedented informational power in the hands of public authorities.

Digital governance does not merely introduce new tools, but it transforms the scale, speed and invisibility of State action. Decisions once taken through human discretion are now embedded in databases, eligibility algorithms and interoperable platforms. Individuals increasingly interact with the State through interfaces rather than institutions, often without clarity on how data is collected, processed, retained or shared. This shift raises foundational constitutional questions about autonomy, dignity, accountability and the limits of executive power.

The Indian Constitution is premised on the idea that State power must remain bounded, contestable and accountable. Articles 14, 19 and 21 collectively impose substantive and procedural restraints on governance. Following *Justice K.S. Puttaswamy v. Union of India*[2], privacy has been recognised as an intrinsic facet of Article 21, grounded in dignity and autonomy. However, subsequent judicial and legislative developments reveal that translating this constitutional recognition into effective institutional restraint has proven uneven and fragile.

Post-*Puttaswamy*[3] jurisprudence reflects a judicial trajectory that oscillates between robust rights-based reasoning and deference to administrative necessity. While the Court has articulated high constitutional standards, necessity, proportionality and procedural safeguards and it has often refrained from subjecting large-scale digital governance projects to sustained structural scrutiny. Parallelly, legislative developments such as the Digital Personal Data

[1] Pallavi Anand, *Enhancing Governance the Digital Way*, The Hindu (last visited Jan. 8, 2026), https://www.thehindu.com/opinion/op-ed/enhancing-governance-the-digital-way/article69069327.ece.
[2] (2017) 10 SCC 1 (India)
[3] *Id.*

Protection Act, 2023[4], while framed as rights-protective, vest wide discretionary powers in the executive, often accompanied by limited parliamentary oversight and weak institutional independence. The result is a growing gap between constitutional principle and regulatory practice.

It is within this context that concerns relating to surveillance, profiling and behavioural regulation emerge. Contemporary data regimes enable forms of observation and categorisation that operate continuously and invisibly, often without explicit coercion. They reshape behaviour by structuring access to welfare, mobility, expression and participation. Surveillance thus appears not as an isolated pathology, but as one dimension of a broader data-driven governance architecture.

George Orwell's *1984* is invoked in this paper not as a literal analogy, but as a conceptual lens to interrogate these structural transformations[5]. Orwell's dystopia illustrates how power can be normalised through routine observation, narrative control and the erosion of private spaces[6]. The relevance of Orwell lies not in predicting authoritarian collapse, but in warning how democracies can gradually internalise techniques of control while retaining constitutional form. Unlike Orwell's telescreens, contemporary digital governance operates through consent frameworks, administrative convenience and invisible infrastructures, making power less visible but no less consequential.

This paper argues that India's emerging digital governance architecture has altered the scale and nature of State power in ways that strain existing constitutional safeguards. By examining key judicial decisions, statutory frameworks and comparative constitutional experience, the study highlights how data-driven governance risks enabling unchecked executive discretion, surveillance normalisation and accountability deficits. Ultimately, it contends that

[4] Digital Personal Data Protection Act, No. 22 of 2023 (India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.

[5] Elif Shafak, *75 Years of 1984: Why George Orwell's Classic Remains More Relevant Than Ever*, LitHub (last visited Jan. 8, 2026), https://lithub.com/75-years-of-1984-why-george-orwells-classic-remains-more-relevant-than-ever/

[6] Orwell's core concepts from *1984* include *telescreens* for constant surveillance, *Thought Police* enforcing self-censorship via psychological manipulation, *Newspeak* limiting rebellious thought through language control, historical revisionism by the *Ministry of Truth*, *doublethink* to accept contradictions and pervasive paranoia dehumanizing citizens under *Big Brother's* watchful eye.

constitutional values - dignity, autonomy, liberty, and constitutional morality must actively shape the design and operation of digital governance.

Knowledge Is Power: Data and the New Governance

Data has emerged as one of the most potent instruments of contemporary governance. Through the systematic collection, aggregation and analysis of personal information, the modern State acquires the capacity to classify populations, predict behaviour and design targeted interventions. Digital technologies enable continuous monitoring at a scale previously unimaginable. Decisions are no longer confined to responding to past conduct but increasingly seek to pre-empt future risks, inefficiencies and dissent. In this sense, data functions not merely as administrative input, but as a central mechanism through which authority is exercised.

In *1984*, power is sustained not primarily through overt violence, but through informational dominance. The Party's authority flows from its capacity to observe citizens continuously and to erase any realm of private thought or action. Contemporary data regimes, though less visible, operate in a strikingly similar fashion. Algorithmic systems enable governance by anticipation, flagging individuals as potential risks, determining eligibility for welfare or subtly shaping behaviour through nudges that operate beneath the threshold of conscious awareness[7].

Indian constitutionalism, however, is premised on the principle of limited government. Articles 14, 19 and 21 collectively impose substantive and procedural restraints on State power. Article 14 prohibits arbitrariness, Article 19 safeguards expressive and associative freedoms, and Article 21 protects life and personal liberty through lawful procedure and due process. These guarantees rest on an assumption that State action is visible, contestable and attributable to identifiable decision makers. Power is constitutionally legitimate only when it can be challenged, justified and reviewed.

Digital governance unsettles these foundational assumptions. Data driven systems often reproduce and amplify existing social inequalities while cloaking discrimination in the

[7] In the United States, the attacks of September 11, 2001 triggered a dramatic expansion of State surveillance powers, most notably through the USA PATRIOT Act (*See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), which broadened the scope of electronic surveillance, data collection and intelligence sharing across agencies. Provisions allowing roving wiretaps, access to business records and secret proceedings before the Foreign Intelligence Surveillance Court significantly lowered thresholds for monitoring private communications in the name of national security. Subsequent disclosures, particularly those arising from Edward Snowden's revelations, exposed the scale of bulk metadata collection conducted by the National Security Agency, reigniting constitutional debate under the Fourth Amendment.

language of technical objectivity. When errors occur, responsibility is diffused across software, databases and administrative hierarchies, leaving individuals without clear avenues for redress. In such an environment, constitutional rights risk being transformed into contingent administrative privileges, granted and withdrawn through opaque processes.

The expansion of surveillance infrastructure in India illustrates this shift. The proliferation of closed-circuit cameras in public spaces, the ubiquity of digital identifiers and the accumulation of mobile, financial and biometric data generate dense digital footprints that are difficult to escape. Surveillance becomes normalised because it is embedded within everyday interactions with the State and the market.

This produces a profound information asymmetry between the State and the citizen. Knowledge thus becomes a mechanism of control. Behavioural regulation operates without the spectacle of repression producing chilling effects[8]. The fear is not of immediate sanction, but of invisible consequences that cannot be predicted or challenged.

The central constitutional question is therefore not whether the State should employ digital technologies, but how such technologies can be reconciled with constitutional limits. Articles 14 and 21 demand that State action be non-arbitrary, proportionate and accountable.

Judicial review must accordingly evolve. Courts must scrutinise not only outcomes but also the processes through which data is collected, analysed and deployed. Transparency, explainability and access to meaningful remedies are essential to preserving constitutional governance in the digital age. Equally important are institutional safeguards. Without such checks, digital governance risks approximating the Orwellian condition of invisible yet omnipresent control.

Privacy as the Last Firewall

The story of privacy in Indian constitutional law is one of delayed recognition and continuing anxiety about the limits of State power. For decades after the Constitution came into force, privacy was not treated as a constitutional value in its own right. The judiciary viewed questions of surveillance and data collection largely through the prism of administrative convenience and public order, reflecting a broader culture of deference to the executive.

[8] Kanakia et.al, *Cambridge Analytica – A Case Study*, 12 Indian J. Sci. & Tech. 1, 1 (2019)

This approach is evident in *M.P. Sharma v. Union of India*[9], where the Supreme Court rejected the very idea of a fundamental right to privacy. The Court held that search and seizure powers under criminal procedure were constitutionally unproblematic and that the Constitution did not protect a general right against State intrusion. Nearly a decade later, *Kharak Singh v. State of Uttar Pradesh*[10] marginally softened this stance. While the Court struck down domiciliary night visits as a violation of personal liberty under Article 21, it upheld other forms of police surveillance. The majority treated surveillance as a routine administrative necessity, whereas Justice Subba Rao's dissent articulated, for the first time, a vision of privacy as integral to dignity and personhood. Yet this dissent remained aspirational rather than authoritative.

Taken together, these early cases reveal a fragmented and underdeveloped privacy doctrine. Constitutional protection was tied to physical intrusion and bodily interference, not to informational control. The constitutional transformation arrived with *Justice K.S. Puttaswamy v. Union of India*[11]. A nine judge bench recognised privacy as a fundamental right intrinsic to life and personal liberty under Article 21 and closely linked to equality under Article 14 and freedom under Article 19. The Court rejected earlier precedents that denied privacy, expressly overruling their restrictive reasoning. Privacy was reimagined as central to dignity, autonomy and the ability to make meaningful choices. Of particular importance was the recognition of informational self-determination, the idea that individuals must retain control over how their personal data is collected, used and shared.

Puttaswamy also supplied a doctrinal framework capable of confronting digital power. Any State action infringing privacy would have to satisfy legality, pursue a legitimate aim, be necessary and pass a strict proportionality analysis with adequate procedural safeguards. Several concurring opinions enriched this foundation[12]. In constitutional terms, *Puttaswamy* represented a principled rejection of an Orwellian State that governs through omnipresent observation.

However, the durability of this protection was soon tested. In *Justice K.S. Puttaswamy v. Union*

[9] M.P. Sharma v. Satish Chandra, 1954 SCR (1) 1077 (India)
[10] Kharak Singh v. State of Uttar Pradesh, 1964 SCR (1) 332 (India)
[11] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India)
[12] *See* Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India) (Chandrachud, J., concurring). Justice Chandrachud conceptualised privacy as spanning bodily, decisional and informational realms. Other judges addressed sexual autonomy, federalism, and the challenges posed by emerging technologies. Drawing on comparative constitutional law, particularly from Germany, Canada and South Africa, the Court demonstrated that privacy evolves through interpretation in response to social and technological change.

of India (Aadhaar)[13] in 2018, the Supreme Court applied the newly articulated privacy doctrine to India's largest digital identity project. The majority upheld Aadhaar for welfare delivery, emphasising fiscal integrity, targeted benefits and administrative efficiency. Certain provisions were struck down and read down, including mandatory linkage with bank accounts and mobile numbers and the use of Aadhaar by private entities. Yet the core architecture of a centralised biometric database was sustained. The dissent, again led by Justice Chandrachud, exposed the constitutional unease underlying the majority's reasoning[14]. This dissent resonates powerfully with Orwell's insight that control flows not from visible coercion but from accumulated knowledge[15]. The Aadhaar judgments thus reveal a judiciary torn between constitutional principle and administrative pragmatism.

Subsequent developments have deepened this tension. Statutes such as the Criminal Procedure (Identification) Act, 2022[16] authorise the collection and long-term retention of biometric data from individuals who may never be convicted of any offence. Surveillance technologies including facial recognition systems and predictive policing tools operate with limited statutory guidance. Databases maintained by agencies such as the National Crime Records Bureau allow data to be retained for decades and shared widely, often without clear purpose limitation or independent oversight. These practices sit uneasily with the proportionality framework laid down in *Puttaswamy*, particularly in the absence of a robust data protection culture.

The evolution of privacy jurisprudence thus mirrors a broader struggle over constitutional power in the digital age. Whether the promise of *Puttaswamy* can withstand the pressures of data centric governance will determine whether privacy remains a living right or fades into symbolic reassurance. In this contest, privacy stands as the Constitution's final defence against

[13] Justice K.S. Puttaswamy v. Union of India (Aadhaar), (2019) 1 SCC 1 (India)

[14] *Id.* (Chandrachud, J., dissenting). He warned that Aadhaar collapsed the distinction between identification and surveillance, enabling the State to assemble comprehensive digital profiles of individuals. Biometrics, he argued, risk transforming citizenship into a condition of permanent legibility, where access to rights depends on continuous authentication.

[15] *Id*. Para 62 of the *Aadhaar case* judgement "On the aforesaid premise, the petitioners point out following heads of challenge: Surveillance: The project creates the architecture for pervasive surveillance and unless the project is stopped, it will lead to an Orwellian State where every move of the citizen is constantly tracked and recorded by the State. The architecture of the project comprises a Central Identities Data Repository (CIDR) which stores and maintains authentication transaction data. The authentication record comprises the time of authentication and the identity of the requesting entity. Based on this architecture it is possible for the State to track down the location of the person seeking authentication. Since the requesting entity is also identified, the activity that the citizen is engaging in is also known violation of Fundamental Right to Privacy"

[16] Criminal Procedure (Identification) Act, No. 11 of 2022 (India), https://www.mha.gov.in/sites/default/files/2022-11/CriminalPro_14112022%5B1%5D.pdf

the quiet emergence of a systemic, unaccountable Big Brother.

Aadhaar as the Constitutional Telescreen

Aadhaar was conceived as a technological solution to long standing failures in welfare delivery, and identity verification. Introduced as a 12-digit unique identity linked to biometric information, it was presented as neutral digital infrastructure rather than a regulatory instrument. Over time, however, Aadhaar has evolved beyond a mere proof of identity into a population scale database embedded across domains such as welfare distribution, banking, taxation and telecommunications. Its constitutional significance therefore lies not only in what it does, but in what it enables.

The constitutional journey of Aadhaar as discussed in the previous section, reflects this transformation. The Court's reasoning rested on a narrow conception of harm, focusing on intention rather than architecture. Aadhaar was evaluated as a scheme in isolation, not as infrastructure capable of indefinite expansion. This stands in contrast to Justice Chandrachud's dissent, which treated Aadhaar as a system of data aggregation with inherent surveillance potential[17].

Data aggregation transforms Aadhaar from identification into governance. Linking across banking, telecom, welfare and digital services collapses silos that once limited State visibility. Consent operates largely as an illusion, as access to essential services becomes contingent on authentication[18]. Authentication failures, biometric mismatches and connectivity issues are treated as technical glitches without identifiable accountability and rarely appear as rights violations.

In *1984*, identity is reduced to a number, anonymity disappears, and individuality dissolves into data. Aadhaar does not constitute Big Brother in itself, but it functions as a potential telescreen. It enables continuous visibility without constant intervention. Citizens are gradually reconstituted as data subjects, legible to the State primarily through databases.

[17] The dissent warned that linking Aadhaar across databases enables profiling, behavioural inference and function creep, where data collected for one purpose is routinely repurposed for others

[18] *From October 1, Only Aadhaar Users Can Book Reserved Train Tickets Online During First 15 Minutes*, The Hindu (last visited Jan. 4, 2026)*, https://www.thehindu.com/news/national/from-october-1-only-aadhaar-users-can-book-reserved-train-tickets-online-during-first-15-minutes/article70053592.ece*

War Is Peace: Surveillance and the Architecture of Permanent Watching

Surveillance law in India has historically been justified through the language of national security, public order and sovereignty. In the pre digital era, this justification was tempered by procedural safeguards. In *PUCL v. Union of India*[19], the Supreme Court held telephone interception required authorisation by a senior executive authority, periodic review by oversight committees and destruction of records once they ceased to be relevant. Even while deferring to security concerns, the Court acknowledged that unchecked surveillance posed a grave threat to privacy and free speech. Digital surveillance has stretched this framework beyond recognition. Surveillance thus operates largely beyond public scrutiny, insulated by claims of national security.

This executive dominance has deep constitutional implications. Surveillance decisions are rarely subjected to adversarial challenge and affected individuals are almost never notified. This creates a trust deficit between citizen and State, where legality is asserted but never demonstrated.

The Pegasus spyware controversy exposed this deficit starkly. Allegations that journalists, activists, and political figures were targeted using military grade spyware raised concerns of extra-legal surveillance[20]. In *Manohar Lal Sharma v. Union of India*[21], the Supreme Court constituted an expert committee. While the committee detected malware on several devices, it could not conclusively attribute responsibility, citing lack of State cooperation. The episode revealed a constitutional blind spot, that surveillance may be technologically sophisticated, yet legally unaccountable.

In Orwell's *1984*, the slogan *War is peace* captures how exceptional measures are normalised through perpetual emergency. Similarly, digital surveillance is defended not as temporary necessity but as continuous precaution. The State no longer waits for wrongdoing, it predicts risk. Predictive policing tools, metadata analysis and algorithmic profiling enable anticipatory governance, where intent is inferred from patterns rather than actions. Metadata plays a central role in this transformation.

---

[19] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India)
[20] Soujaatyaa Roy, *The Impact of the Recent Pegasus Spyware Controversy on the Right to Privacy in India*, 6 Int'l J.L. Mgmt. & Human. 1060 (2023)
[21] Manohar Lal Sharma v. Union of India, W.P. (Crl.) No. 314 of 2021 (India)

Digital tracking of protests and dissent further illustrates this tension. Monitoring of online speech, social media mapping and location tracking create chilling effects. Individuals modify behaviour not because they are punished, but because they anticipate being watched. In Orwellian terms, *thoughtcrime* begins in silence. Initiatives such as the Sanchar Saathi portal exemplify this shift. Framed as cyber security infrastructure, it uses algorithmic tools to detect suspicious SIM usage and digital patterns[22]. While courts have articulated privacy as a fundamental right, the lack of a comprehensive surveillance law means that constitutional standards remain largely unenforced in practice[23].

The DPDP Act, 2023: Data Protection or Statutory Normalisation of Surveillance

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first attempt at a comprehensive statutory framework governing the processing of personal data. Enacted in the aftermath of *K.S. Puttaswamy v. Union of India*, the Act purports to translate constitutional recognition of informational privacy into regulatory form. On its face, the statute incorporates familiar data protection principles, that is consent-based processing, purpose limitation, data minimisation and accountability of data fiduciaries.

Yet, when examined through a constitutional lens, the DPDP Act reveals a troubling asymmetry between private obligations and State power. While private entities are subjected to detailed compliance duties, the State enjoys expansive exemptions grounded in broadly framed interests such as sovereignty, security of the State, public order and friendly relations with foreign States. More significantly, the Act empowers the executive to exempt entire classes of data processing through notification, effectively allowing privacy protections to be suspended without parliamentary deliberation or judicial scrutiny[24]. Orwell's concern in *1984* was not merely surveillance conducted in secrecy, but surveillance that is routinised, legalised and justified as necessary for collective security[25].

The absence of a genuinely independent oversight mechanism compounds this problem. The

[22] Sanchar Saathi, Government of India, https://www.sancharsaathi.gov.in/ (last visited Jan. 5, 2026)
[23] *The Indian Surveillance Framework and the Centre's Surveillance Order: Addressing Challenges to Individual's Right to Privacy*, 2 Madras L.J. 1 (2020)
[24] *Data Protection Rules and Act a Net Negative for Privacy Rights*, The Hindu (last visited Jan. 9, 2026), https://www.thehindu.com/opinion/op-ed/data-protection-rules-and-act-a-net-negative-for-privacy-rights/article69212801.ece
[25] George Orwell, 1984 (Secker & Warburg 1949). *The Party does not apologise for watching; it normalises observation as the condition of social order.*

Data Protection Board is structurally dependent on the executive, lacking the institutional autonomy typically associated with constitutional watchdogs. This concentration of power raises serious concerns under Article 14, which guards against arbitrariness and demands non-capricious State action. When the same State that collects, processes and aggregates personal data also controls the mechanisms of supervision and enforcement, the promise of accountability becomes illusory.

Consent, positioned as the normative foundation of the DPDP Act also warrants sceptical scrutiny. In practice, consent often operates in conditions of severe power asymmetry that is by employing take-it-or-leave-it digital services, welfare conditionalities and platform monopolies leave individuals with little meaningful choice. Orwell's dystopia captures this paradox through the idea of *voluntary obedience*[26]. Consent without bargaining power, transparency or alternatives cannot meaningfully be equated with autonomy, which *Puttaswamy* recognised as central to dignity under Article 21.

Comparative Constitutional Responses

The European Union conceptualises large-scale data collection through a fundamentally rights-based constitutional lens. Big data, while acknowledged as useful for security and governance, is treated as a structural risk when accumulated without strict legal controls. This approach reflects Europe's historical experience with authoritarian surveillance and its resulting scepticism of unchecked executive power. In *Big Brother Watch v. United Kingdom*[27], the European Court of Human Rights accepted that national security may justify bulk interception but held that such regimes violate democratic values unless accompanied by rigorous safeguards. Independent prior authorisation, continuous oversight and effective remedies were identified as constitutional necessities, not optional protections.

These values are further operationalised through the General Data Protection Regulation[28]. While not a surveillance statute, the GDPR embeds constitutional principles like purpose

[26] *Id*.Citizens appear to consent, but dissent is structurally foreclosed.
[27] Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R. (Sept. 13, 2018).
[28] Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]; *see also* GDPR-info.eu, https://gdpr-info.eu/ (last visited Jan. 10, 2026). The General Data Protection Regulation embodies a rights centric model of data governance, emphasising purpose limitation, data minimisation, transparency and individual control. While the GDPR is not a surveillance statute per se, it constrains how data can be collected, retained and repurposed by both State and private actors.

limitation, data minimisation, transparency and individual control into everyday data governance. By restricting how data may be collected, retained and repurposed, the EU demonstrates that administrative efficiency need not depend on limitless data accumulation.

In the United States, constitutional engagement with digital surveillance has evolved more gradually, particularly in the aftermath of 9/11. Early jurisprudence displayed marked deference to executive claims of national security. Over time, however, the Supreme Court acknowledged that digital technologies fundamentally alter the nature of surveillance.

In *Carpenter v. United States*[29], the Court held that long-term access to historical cell-site location information constitutes a search under the Fourth Amendment, requiring judicial authorisation. Rejecting the argument that such data were mere business records, the Court recognised that aggregated digital information reveals intimate patterns of life. Similar concerns animated *Riley v. California*[30], where warrantless smartphone searches were barred due to the unparalleled depth of personal information stored on digital devices.

The American constitutional trajectory also illustrates doctrinal evolution. Early decisions such as *Olmstead v. United States*[31] upheld wiretapping absent physical trespass, a position later overturned by *Katz v. United States*[32], which introduced the reasonable expectation of privacy standard. This shift laid the foundation for modern informational privacy jurisprudence, demonstrating that constitutional protections must adapt to technological change to remain meaningful. China represents a contrasting model, where data is explicitly treated as a strategic national resource. State-controlled data marketplaces in cities such as Shenzhen, Guiyang and Shanghai seek to formalise data ownership, valuation and exchange, often using blockchain-based trust mechanisms[33]. These platforms facilitate transactions involving public datasets and AI training data, while maintaining strict government oversight. Australia grapples with big data concentrating power in a few tech giants, enabling unchecked surveillance, interference and kinetic threats while outpacing weak regulations[34].

[29] Carpenter v. United States, 585 U.S. 296 (2018)
[30] Riley v. California, 573 U.S. 373 (2014)
[31] Olmstead v. United States, 277 U.S. 438 (1928)
[32] Katz v. United States, 389 U.S. 347 (1967)
[33] Alex He et al., *Data Marketplaces and Governance: Lessons from China*, in The Role of Governance in Unleashing the Value of Data 61 (Ctr. for Int'l Governance Innovation 2024), http://www.jstor.org/stable/resrep64581.12 (last visited Jan. 5, 2026)
[34] Miah Hammond-Errey, *Big Data and National Security: A Guide for Australian Policymakers* (Lowy Inst. for Int'l Pol'y 2022), https://www.jstor.org/stable/resrep39703 (last visited Jan. 11, 2026)

Big data is a 21st century arms race in which States compete to control vast datasets for security and law enforcement, often at the cost of privacy. It is clear that cross-border nature of data generates conflicts of law, especially between the European Union's rights-based data protection regime and the United States' security-driven, sectoral approach[35]. While contexts differ, such models challenge the assumption that efficiency requires maximal data concentration. However across jurisdictions, a common constitutional thread emerges. Surveillance is tolerable only when embedded within legality, necessity, proportionality and oversight. Independent authorisation, transparency and remedies are democratic necessities, not procedural luxuries. From an Orwellian standpoint, comparative jurisprudence underscores what is at stake. Orwell's dystopia is not defined by technology alone, but by institutional collapse.

Other Concerns

Beyond questions of legality and proportionality, India's digital governance framework raises serious concerns regarding data security, informational asymmetry and the human costs of systemic breaches. Repeated instances of data theft have undermined claims that State-held databases are inherently safer than private repositories. As early as 2018, Aadhaar enrolment data was reportedly sold online for nominal sums[36]; in 2023, the CoWIN portal exposed sensitive vaccination records[37]; and in 2024, SIM-swap frauds enabled unauthorised access to Aadhaar-linked services. These breaches vindicate long-standing critics who warned that centralised identity architectures create single points of failure with cascading constitutional consequences.

The Digital Personal Data Protection Act further exacerbates informational asymmetry. Its broad exemptions for reasons of public order and national security risk enabling targeted narratives and data-driven propaganda without meaningful oversight. This concern is not abstract. Allegations surrounding data analytics and political messaging during the 2019 general elections, often compared to the Cambridge Analytica episode, highlight how personal

[35] Els De Busser, *Big Data: A Twenty-First Century Arms Race* (Ctr. for Int'l Governance Innovation), http://www.jstor.com/stable/resrep03719.5 (last visited Jan. 11, 2026)
[36] Randeep Ramesh, *India National ID Database Data Leak Bought Online, Raising Privacy Fears*, The Guardian (Jan. 4, 2026), https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar
[37] *Explained: What Does the Alleged CoWIN Data Leak Reveal?, The Hindu (Dec. 27, 2025), https://www.thehindu.com/sci-tech/technology/explained-what-does-the-alleged-cowin-data-leak-reveal/article66980831.ece*

data can be weaponised to influence democratic choice[38]. The rise of deepfakes and synthetic media further complicates this landscape, destabilising truth itself.

Crucially, contemporary surveillance is co-produced by the State and private platforms. Data-sharing mandates, platform compliance obligations and the role of telecom and fintech intermediaries blur the public–private divide, raising unresolved questions about the horizontal application of fundamental rights and State responsibility through delegation.

India increasingly uses artificial intelligence to improve governance, from real-time translation that bridges linguistic diversity to chatbots and predictive tools in welfare delivery[39]. AI is also reshaping cybersecurity. Attacks are no longer limited to individual hackers but are driven by organised ransomware groups and even state-backed actors who lock or manipulate data rather than merely stealing it. Digital governance depending on algorithmic systems are not objective. They replicate and amplify existing social biases embedded in data, design choices, and institutional priorities[40]. Many algorithmic models lack explainability, preventing individuals from understanding how decisions are made. India's breach governance remains weak[41]. Disclosures under the Information Technology Act and CERT-In rules contrast with global norms[42] (unlike GDPR's 72 hours).

Public data is essential for AI innovation. However policymakers must clearly define what qualifies as public data. Without clear limits on how such data may be used or disclosed, its use can fall into legal and ethical grey areas. Ultimately, public does not mean permissionless[43]. In light of the above discussed concerns, India needs a balanced path blending rights with progress.

Conclusion: Future trajectory

At a deeper level, the challenges examined in this paper point to the emergence of what may

[38] *What Did Cambridge Analytica Do During the 2016 Election?*, NPR (Jan. 20, 2026), https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election
[39] *Six Ways Government of India Uses AI for Governance*, IndiaAI (India Artificial Intelligence Portal) (Jan. 20, 2026), https://indiaai.gov.in/article/six-ways-government-of-india-uses-ai-for-governance
[40] Emilio Ferrara, *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies*, 6 Sci. 3 (2024)
[41] *Data Breach Reporting*, DPO-India (Data Protection Officer India), https://dpo-india.com/Blogs/data-breach-reporting/#globalsurvey (last visited Jan. 20, 2026)
[42] *India's 6-Hour Data Breach Reporting Rule*, UpGuard (Blog), https://www.upguard.com/blog/indias-6-hour-data-breach-reporting-rule (last visited Jan. 20, 2026).
[43] *Scraping Public Data in India: Innovation Enabler or Privacy Threat?*, Int'l Ass'n of Privacy Pros. (IAPP) (Jan. 2, 2026), https://iapp.org/news/a/scraping-public-data-in-india-innovation-enabler-or-privacy-threat-

be described as the Fourth generation of human rights, rights that respond not to physical coercion or formal discrimination, but to informational power, algorithmic control and the ability of States and corporations to predict, shape and pre-empt human behaviour. Privacy, data protection and informational autonomy are no longer ancillary interests. They are foundational conditions for the exercise of liberty, equality and democratic participation in a digital society. Data-driven governance has altered not merely how the State administers welfare, security and public services, but how power itself is exercised and experienced. Aadhaar-linked welfare delivery, predictive governance tools, surveillance technologies and the Digital Personal Data Protection Act, 2023 collectively promise efficiency, inclusion and rational administration. Yet this paper has shown that these same systems also concentrate informational power in ways that strain constitutional guarantees.

History offers an unsettling reminder that surveillance has rarely remained benign. Long before Orwell, states relied on intelligence networks to discipline dissent. What distinguishes the present moment is scale, speed, and invisibility. Compounding this threat is the rise of private surveillance. Corporations now collect and monetise personal data on a scale that exceeds even Orwell's imagination. Search histories, social media interactions, health metrics and location data are transformed into predictive products, influencing insurance pricing, credit access, political messaging and consumer behaviour.

Post-*Puttaswamy* jurisprudence correctly recognises privacy as intrinsic to dignity and autonomy under Article 21. However, the translation of this principle into lived protection remains uneven. The DPDP Act adopts the language of consent, data minimisation and accountability, but simultaneously entrenches sweeping executive exemptions and weak oversight structures.

Comparative constitutional experience underscores what is missing. These systems are far from perfect, but they demonstrate that security and strong privacy protections are not mutually exclusive. This is where Orwell's warning becomes most relevant. The danger is not the spectacle of totalitarian repression, but the slow acceptance of surveillance as lawful, normal and inevitable.

A meaningful constitutional response must therefore be structural and forward-looking. Judicial oversight of surveillance must be strengthened, with warrant requirement enforced as a universal baseline rather than a dispensable formality. Surveillance should be treated as an

extraordinary intrusion, justified only by necessity and subjected to independent authorisation. India also requires a genuinely independent Data Protection Authority, insulated from executive control, with security of tenure, enforcement powers and transparency obligations.

Equally important is algorithmic accountability. Article 14 demands mechanisms to audit algorithms for bias, arbitrariness and opacity. Surveillance and data retention laws must incorporate meaningful sunset clauses to prevent emergency measures from becoming permanent features of governance. The relationship between the right to information and the right to privacy must be recalibrated so that secrecy does not function as a blanket shield against democratic scrutiny[44].

Ultimately, digital constitutionalism must remain anchored in dignity, liberty and constitutional morality. Courts, legislatures, regulators and citizens all have roles to play. Parliamentary oversight committees, mandatory data protection impact assessments and public participation are essential complements to judicial review. India is NOT Orwell's Oceania. Yet unchecked data power risks hollowing constitutional promises from within. Orwell reminds us that freedom is often lost not through dramatic collapse, but through gradual accommodation. The Constitution must ensure that Big Brother remains a warning and not a design choice.

[44] *Too Little, Much Later: On the Digital Personal Data Protection Rules, 2025*, The Hindu (Jan. 7, 2026), https://www.thehindu.com/opinion/editorial/too-little-much-later-on-the-digital-personal-data-protection-rules-2025/article70287191.ece

References

Books

1. George Orwell, 1984 (Secker & Warburg 1949).

2. V.N. Shukla, Constitution of India (Eastern Book Co. 2019).

3. Aleksei Pavlichev & G. David Garson, Digital Government: Principles and Best Practices (Routledge 2003).

4. Gautam Bhatia, The Transformative Constitution (Oxford Univ. Press 2019).

5. Benjamin J. Goold & Liora Lazarus, Security and Human Rights (Hart Publishing 2007).

6. Nandan Kamath Ryder & C.S. Naren, Artificial Intelligence and Law: Challenges Demystified (Law & Justice Publishing 2022).

Journals/Articles

1. Kanakia et al., *Cambridge Analytica — A Case Study*, 12 Indian J. Sci. & Tech. 1 (2019).

2. Soujaatyaa Roy, *The Impact of the Recent Pegasus Spyware Controversy on the Right to Privacy in India*, 6 Int'l J.L. Mgmt. & Human. 1060 (2023).

3. Miah Hammond-Errey, *Big Data and National Security: A Guide for Australian Policymakers* (Lowy Inst. for Int'l Pol'y 2022), https://www.jstor.org/stable/resrep39703 (last visited Jan. 11, 2026).

4. Els De Busser, *Big Data: A Twenty-First Century Arms Race* (Ctr. for Int'l Governance Innovation), http://www.jstor.com/stable/resrep03719.5 (last visited Jan. 11, 2026).

5. Randeep Ramesh, *India National ID Database Data Leak Bought Online, Raising Privacy Fears*, The Guardian (Jan. 4, 2018), https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar (last visited Jan. 4, 2026).

6. Emilio Ferrara, *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies*, 6 Sci. 3 (2024).

7. Susan Ariel Aaronson, *What Kinds of Threats Are Posed by Inadequate Governance of Personal Data?*, in Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves (Ctr. for Int'l Governance Innovation 2020).

8. G. Jujjavarapu, *India: New Laws Needed to Protect Citizens from Invasive Profiling*, Internet Pol'y Rev. (Feb. 21, 2017).

9. Mark J. Taylor & Jeannie Marie Paterson, *Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection*, 16 Indian J.L. & Tech. 4 (2020).

10. Mark Linscott & Anand Raghuraman, *Aligning India's Data Governance Frameworks* (Atlantic Council 2020).

11. *The Indian Surveillance Framework and the Centre's Surveillance Order: Addressing Challenges to Individual's Right to Privacy*, 2 Madras L.J. 1 (2020).

12. Rashmi S. Patil, *Surveillance and Control in George Orwell's "1984": A Critical Insight*, 10 Int'l J. Eng. Literature & Soc. Sci. 207 (2025).

Internet Sources

1. Shreya Tewari, *India's Data Protection Bill, 2019 — The Beginning of an Orwellian Era*, Penn Carey Law: J.L. & Soc. Change, https://www.law.upenn.edu/live/news/9748-indias-data-protection-bill-2019-the-beginning-of (last visited Jan. 8, 2026).

2. Elif Shafak, *75 Years of 1984: Why George Orwell's Classic Remains More Relevant Than Ever*, LitHub, https://lithub.com/75-years-of-1984-why-george-orwells-classic-remains-more-relevant-than-ever/ (last visited Jan. 8, 2026).

3. *What Did Cambridge Analytica Do During the 2016 Election?*, NPR, https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election (last visited Jan. 20, 2026).

4. *Six Ways Government of India Uses AI for Governance*, IndiaAI (India Artificial Intelligence Portal), https://indiaai.gov.in/article/six-ways-government-of-india-uses-ai-for-governance (last visited Jan. 20, 2026).