INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

SURVEILLANCE AND SOVEREIGNTY; STRIKING A BALANCE IN THE DIGITAL AGE

AUTHORED BY - ANUJA CHOUDHURY & SRI SNIGDHA

I. ABSTRACT

The rapid digitalisation of society at large has intensified the dynamic of data privacy and state surveillance, giving raise to significant questions regarding the rights of an individual and national security. This Article mainly examines the evolving framework of the Indian Legislature, primarily concentrating on the Information Technology Act, 2000[1] and the Digital Personal Data Protection Act, 2023[2]; the cornerstones of the legislations governing data privacy in India. The study explores landmark precedents, especially the decision upheld by the hon'ble Supreme Court in K.S. Puttaswamy vs Union of India[3], which lead to the recognition of Privacy as a Fundamental Right, further analysing important judicial decision of PUCL vs Union of India.[4] The Article concentrates on certain provisions within the DPDP Act[5] and the IT Act[6], which permit the government "exemptions" on basis of sovereignty, security or public order, undermining the spirit of privacy rights of an individual. Further, the Article concentrates on the loopholes in the statutes. The research provides with a comparative analysis with India and Southeast Asian countries like China and Singapore, delving deeper into the differences between the three countries. Ultimately, the article evaluates the bridge between data privacy and state surveillance, providing a detailed explanation on the consensus of both. Ultimately, the article calls for substantive reforms to ensure that state surveillance is justified, limited, and accountable in a democratic economy such as India. The work concludes by promoting a consensus driven approach, keeping in mind the interests of the state and the privacy rights of citizens, in alignment with global practices, while sustaining the key constitutional values.

[1] (Information technology act, 2000) <https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf> accessed 1 September 2025

[2] (The Digital Personal Data Protection Act, 2023 ...).<https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> accessed 31 August 2025.

[3] (Justice K. S. Puttaswamy - Digital Supreme Court reports) <https://digiscr.sci.gov.in/view_judgment?id=NjEwMg%3D%3D> accessed 23 August 2025.

[4] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

[5] Ibid (n 2).

[6] Ibid (n 1).

ISSN: 2582-6433

Keywords: Data Privacy, State Surveillance, IT Act, 2000, DPDP 2023, Southeast Asian Countries.

II. INTRODUCTION

The balance between the Right to Privacy and state surveillance remains one of the unresolved legal and ethical challenges of the current modern era. Rapid technological advancements, unprecedented data generation, and the heavy reliance on surveillance tools and systems have all contributed to the ongoing debate over the fundamental right to privacy and the limitations of the government.

The Hon'ble Supreme Court in the case of *K.S. Puttaswamy Vs Union of India*[7] has upheld the Right to Privacy as a Fundamental Right. It has served as the beginning of further legislative developments in India, such as the Digital Personal Data Protection Act (DPDP), 2023[8], being one of the significant among others. The DPDP Act strengthens an individual's control over their personal information by imposing certain mandates such as explicit consent, data minimisation requirements, and other important features such as access and erasure. Another pre-existing statute before the DPDP Act is the Information Technology Act, 2000 and the subordinate of the IT Act, 2000, the IT Rules[9], both of which establish a regulatory structure for data protection, though there are certain loopholes that the IT Act, 2000, does not address. Despite the introduction of many data privacy statutes, India's surveillance still has certain grey areas that have to be addressed. Over the years, the growing use of technology has driven the legislature to form laws for addressing the legal framework the prevent any misuse of data by any individual. [10]Yet, certain necessities of the state lead to the rise of intercepting data for national security and keeping in mind other interests of the country. These exemptions and powers given to the state lead to the bridge between individuals and the state, creating a sense of distrust in the minds of people.

This Article focuses on the interplay between data privacy and state surveillance, concentrating on key legislation such as the DPDP Act, the IT Act, a comparative study between India and

[7] (Justice K. S. Puttaswamy - Digital Supreme Court reports) <https://digiscr.sci.gov.in/view_judgment?id=NjEwMg%3D%3D> accessed 1 September 2025.
[8] Ibid (n 2).
[9] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf accessed 24 August 2025
[10] Indian Telegraph Act 1885 (India) s 5 https://indiacode.nic.in/handle/123456789/14917#section-5 accessed 2 August 2025.

ISSN: 2582-6433

other countries in the Southeast region, and finally, the emerging consensus between Data Privacy and State surveillance. Through different case analyses and the detailed study of challenges faced, the article discusses critical issues that shape data governance in India.

III. INFORMATION TECHNOLOGY ACT, 2000

The need for an IT Act emerged due to the constant growth of cyberspace and technology from the mid-90s. Though computers were used in important offices and other places, the growth of technology boomed in the past one and a half decades, wherein the turn of the tech world took a sharp and notable curve in the history of the world, not pertaining to India alone. This fast-paced growth of technology needed a new boundary of its own to regulate the law and prevent it from any misuse. The demand for an alternative to paper was placed on the international agenda, and India, being a part of the UN, had to take up the resolution passed by the UNIDRIL in 1984, which was to develop a 'Model Law' for electronic commerce. The IT Act, 2000, was nothing but an outcome of this International Commitment.

The word '*information*' has been defined in Section 2(1)(v) of the IT Act, 2006[11] as, "Information includes data, text, images, sound, voice, codes, computer programs, software and databases or microfilm or computer-generated microfiche". The Law of evidence is traditionally based on paper-based records and oral testimony. As electronic commerce eliminates the need for paper-based transactions, the need for legal changes has become a necessity. Globalisation, which had emerged in the late 90s, started to erase the boundaries that were initially set, and raised the need for legal recognition of technology across borders, especially due to the involvement of the developed nations. The alarming magnitude of issues rising, especially within India and out of India, the need for a law.

The parliament passed the IT Act, 2000 on 15th May, 2000, it was approved by the then president in June 2000 and was enforced on October 17, 2000. The provision of the IT Act is not only applicable in India but also for the offences committed overseas by an Indian citizen, The IT Act, 2000, is the basic law that regulates all digital activity and cybersecurity issues in India. Over the course of time, the IT Act has evolved with time, now enforcing necessary laws relating to electronic transactions, cybercrimes, data privacy and protection among many other

[11] (India code: Section details) <https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&=&sectionId=13011&=&sectionno=2&=&orderno=2> accessed 1 September 2025.

ISSN: 2582-6433

functions.[12] One of the major uses and advantages of the IT Act, 2000 is the strong legal framework that is established for electronic governance, digital signatures, and other cybercrime-related procedures, which boosts India's need for reliance in the digital sector, and marks a sense of trust in the new digital economy. Through provisions such as Section 69, 69A and 69B of the IT Act, 2000[13], which empower the government to issue directions for interception, monitoring or decryption of any information through any computer source.

The I.T. Act, 2000, defines the following types of crimes:

1. Hacking
2. Denial of Service
3. Virus Dissemination
4. Fraud
5. Phishing
6. Cyber Stalking

The IT Act mainly speaks about state surveillance but does not emphasise private actor surveillance, also it ignores the surveillance of mass surveillance, targeted surveillance and lateral surveillance. There is no judicial oversight as the interception orders are approved by the executive authorities, which means that the same branch of government that requests approval is accepting the orders, which states the lack of accountability of the executive in such situations. Section 69(1) of the IT Act, 2000[14] states that in unavoidable circumstances, any authorised officer can approve interception or monitoring without any prior approval, which can be a serious cause of misuse, and there is no proper definition of unavoidable circumstances, which makes it subjective and ambiguous. The IT Act and IT Rules mainly focus on the private bodies, which, in a way, gives leeway to the government organisations, which might lead to a lack of accountability and responsibility for any individual who has the private information of many people in their hands. If an individual is taken under surveillance for any security purpose, and is not found guilty of any misuse or any such action which might be considered harmful, he or she is not notified of the fact that they were under surveillance, which keeps individuals in the dark. The Review Committee under the IT Rules itself is

[12] (RMLNLU) <https://www.rmlnlu.ac.in/> accessed 1 September 2025.
[13] (Section 69) <https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=88> accessed 30 August 2025.
[14] Ibid (n 13).

ISSN: 2582-6433

composed of government officials, which undermines the process of checks and balances in a democratically functioning country like India.

IV. EVOLUTION OF DPDPA, 2023

In today's data-driven world, the protection of personal information has become a global priority. These data mustn't be used for economic interest by the government. If compared with the last century, in modern-day India, a significant digital transformation can be observed. However, alongside these advancements, misuse of the technology and rise in cybercrimes have also increased.

Although not explicitly mentioned in the Constitution about the right to privacy, it has been included under Article 21[15] of the Indian Constitution by various Supreme Court judgments. The said freedom has also undergone various judicial judgments and has evolved into a primary right of the citizens, which is a fundamental right in recent ages.

The pivotal case that reshaped privacy laws in India was *K.S. Puttaswamy and Anr. v. Union of India and Ors.*[16] *(2017).*[17] Here, a retired high court judge of Madras questioned the constitutional validity of the Aadhaar scheme, where the government wanted to collect biometric and geographic data. This scheme leaked the personal information of millions and highlighted the vulnerabilities and flaws in India's data privacy safeguards. Subsequently, a nine-judge bench was constituted to look into the issue. The key legal question that came up was the validity of the right to privacy and whether it comes under the Constitution of India. In this landmark judgement, the apex court overruled the previous judgements of *Kharak Singh v. State of MP (1961)*[18] *and Gobind vs. State of MP & Anr (1975)*[19], affirming that the privacy right is a fundamental right and laid the groundwork for the DPDP Act 2023 and DPDP Rules 2025, a comprehensive data protection law that India lacked.

[15] Constitution of India, Part III - Fundamental Rights (Ministry of External Affairs) https://www.mea.gov.in/images/pdf1/part3.pdf accessed 20 August 2025.
[16] Ibid (n 7).
[17] (Justice K. S. Puttaswamy - Digital Supreme Court reports) <https://digiscr.sci.gov.in/view_judgment?id=NjEwMg%3D%3D> accessed 21 August 2025.
[18] 'Right to Privacy: Court in Review' (SC Observer, Year) https://www.scobserver.in/journal/right-to-privacy-court-in-review/ accessed 21 August 2025.
[19] Aisika Basu, 'Govind v State of Madhya Pradesh: A legal analysis' (2022) 3 Jus Corpus Law Journal https://www.juscorpus.com/wp-content/uploads/2022/11/152.-Aisika-Basu.pdf accessed 11 August 2025.

ISSN: 2582-6433

Due to the several challenges the government faces, the government had a duty to prioritise individual privacy rights. Therefore, on July 31, 2017, a ten-member expert committee under the chairmanship of Justice (Retd) BN Srikrishna was appointed to recommend key principles to uphold personal privacy and data rights of people in India.[20] The recommendations given by this committee resulted in the development of a robust data protection act.[21]

Earlier, India relied on older privacy laws like the IT Act, 2000 and the Telegraph Act, 1885. Later, with cabinet approval, the DPDP bill was passed in the Lok Sabha. This act holds a comprehensive and detailed legislative structure to collect, store and govern the personal information of individuals.[22] It is an applicable measure taken by the government of India, demonstrating the government's commendable effort and approach to secure data sovereignty while promoting economic progress amid rapid globalisation. The Act empowers citizens with limited authority to manage and control their data and builds trust and confidence in the government. The Digital Personal and Data Protection (DPDP) Act[23] primarily makes sure that citizens continue to have authority over their data while also holding entities accountable for their misdeeds. Section 6[24] of the Act emphasises the necessity of obtaining free, specific, informed, unconditional and unambiguous consent before their data is processed.[25] The reason behind collecting one's data also needs to be explained to the individual, and they have the choice to accept or deny it without any force or coercion. Whereas, Section 8[26] maps out the duties of the data fiduciary, any person or organisation, like the bank or hospital, that decides the purposes and methods of using the personal data. This section says that it is their job to ensure that the individuals are informed about their data collection and also to set up proper grievance redressal mechanisms. The legislature also permits cross-border data transactions unless it is a black listed nation by the Union government. Special rules are also mentioned for children and persons with disability. The

[20] https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy accessed 22 August 2025.
[21] Economic Laws Practice, 'Justice BN Srikrishna Committee - White Paper on Data Protection' (December 2017) https://elplaw.in/wp-content/uploads/2023/09/ELP-Discussion-Paper-Justice-BN-Srikrishna-Committee-Data-Protection-2.pdf accessed 27 August 2025.
[22] https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en&utm_source=chatgpt.com accessed 25 August 2025.
[23] Ibid (n 2).
[24] Digital Personal Data Protection Act, 'Chapter 2, Section 6: Consent' (2025) https://dpdpa.com/dpdpa2023/chapter-2/section6.html accessed 24 August 2025.
[25] AZB & Partners, 'Digital Personal Data Protection Act, 2023 – Key Highlights' (AZB & Partners, August 2023) https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/ accessed 15 August 2025.
[26] Digital Personal Data Protection Act, 'Chapter 2, Section 6: Consent' (2025) https://dpdpa.com/dpdpa2023/chapter-2/section6.html accessed 24 August 2025.

ISSN: 2582-6433

penalties are also very harsh, which can go up to 250 crores, depending upon the nature of the breach.[27]

Despite this act being such a success in the Indian technological era, legal scholars and privacy experts have expressed grievances and warnings that certain provisions may not completely reflect the constitutional privacy standards that were outlined in the K.S. Puttaswamy case[28]. They point out that wide government exemptions, fewer user rights in some cases and the absence of an independent regulator could weaken the privacy protections promised by the Supreme Court.

Although the DPDP Act is considerably more progressive, it also has its shortcomings. For instance, one major issue is the transfer of data abroad. Although it allows for it, there are no clear rules or consequences stated in the act if companies fail to comply. With a lot of importance given to informed consent, it permits few institutions like schools and childcare facilities to monitor children for certain purposes and persons with disabilities, there are no specific guidelines mentioned, weakening their rights to file complaints. Another critical issue is not giving enough independence to the Data Protection Board (DPB). It is not fully autonomous, given that they are funded by the government and the members are appointed by the central government.[29] Additionally, with only one office in Delhi, this creates many more problems for the rural people, as they struggle to access remedies. At last, the federal framework of the nation adds complexities, as state-level data concerns are also governed by the union, which creates potential conflict and mistrust.

In the matter of *Karthick Theodore v. Registrar General*, [30]the appellant was charged under sections 417 and 376 IPC. Although the appellant was convicted by the trial court, he was later released by the Madras High Court. The appellant's main contention was that, even after his acquittal, his case was still displayed on High Court websites and various legal databases. This

[27] Right to Privacy, Evolution, Significance, Challenges' (Vajiram and Ravi, August 2025) https://vajiramandravi.com/upsc-exam/right-to-privacy/ accessed 18 August 2025.
[28] Sujeet Katiyar, 'Justice K.S. Puttaswamy Judgment: Foundation of India's Data Protection Law' (LinkedIn, 2023) https://www.linkedin.com/pulse/justice-ks-puttaswamy-judgment-foundation-indias-data-sujeet-katiyar-gisyf accessed 21 August 2025.
[29] Internet Freedom Foundation, 'The Digital Personal Data Protection Bill 2022 Does Not Satisfy the Supreme Court's Puttaswamy Principles' (Internet Freedom Foundation, 2022) https://internetfreedom.in/the-digital-personal-data-protection-bill-2022-does-not-satisfy-the-supreme-courts-puttaswamy-principles accessed 25 August 2025
[30] Karthick Theodore v Registrar General W.A.(MD) No.1901 of 2021, Madras High Court (27 February 2024).

ISSN: 2582-6433

posed a harm in professional and personal life, as when he applied for an Australian visa for work, online searches still associated his name with criminal charges. This caused social stigma as he could not move forward with his name being showcased on the public records with criminal charges. Later, he sought a writ of mandamus asking the High Court to remove his name from the record and instruct the databases to update their records.

However, the High Court dismissed the petition, ruling that the High Court is an open court and court of record as mentioned under Article 215 of the Constitution[31] and is barred from changing any sort of judicial record unless authorised by the law. The court also observed that the digital protection rules outlined in this law exclude courts from Section (17)(1)(b)[32] erasure duties, as open justice and transparency are given more priority than upholding privacy in cases like these.

Despite the rules mentioned in the act, which are supposed to protect one from the state regulations and safeguard their privacy, this case highlights its drawbacks and gives a hint that no act is absolute, and even though we have been given the authority to have control over our data in a way, it is not ultimate. The appellant here, though he was acquitted of all the charges, his name was not redacted from the public judicial records, obstructing his life decisions later. This clarifies that, no matter how important it is for the citizens to remove their digital footprints, the state and law will always play a bigger role. This also emphasises how stronger legislation is needed, where open justice and privacy of personal details need to be put in equilibrium to further prevent such acquitted individuals from going through lifelong penalties, such as visa denials or harm to one's reputation in today's digital age. [33]

V. STATE SURVEILLANCE AND CONSENSUS

In simplest words, the word state surveillance means when the government engages in gathering and monitoring personal information for various purposes, such as national security, to prevent terrorism or any external aggression, or for public safety and administrative

[31] Moushumi Bhattacharya, 'Article 215 of the Constitution of India empowers the High Court to review its judgments – Calcutta HC' (SCC Online Blog, 5 September 2023) https://www.scconline.com/blog/post/2023/09/05/article-215-constitution-empowers-hc-review-its-judgments-calcutta-hc-scc-blog-legal-research/ accessed 21 August 2025.
[32] Digital Personal Data Protection Act 2023 (India) s 17 https://dpdpa.com/dpdpa2023/chapter-4/section17.html accessed 24 August 2025.
[33] Aman Avinav, 'DPDP Rules Inch Forward but Bring Challenges' (Law.asia, 2025) https://law.asia/digital-personal-data-protection-rules-challenges-india/ accessed 14 August 2025.

ISSN: 2582-6433

purposes, like keeping a track of population data. The emergence of state surveillance comes from the French philosopher Foucault's theory of surveillance. He gave the concept of panopticism, which is still relevant in modern society.[34] He was inspired by Jeremy Bentham's prison design, which was called the panopticon, a circular prison with a watchtower in the middle. This was done to discipline the prisoners without placing guards in every cell, to ensure that the prisoners behave accordingly, as they will know that they are being watched continuously. His idea inspired many modern societies to use surveillance and control.

Surveillance in India has improved through the years alongside technological advancements. Historically, India has always struggled to balance surveillance with respect for privacy. The laws passed by the British government to keep tabs on communications continued to exist until the *PUCL vs. Union of India*[35] judgment ruled out certain laws and declared the rest to be illegal or extreme state control.

To comprehend surveillance, it is important to study its various types that India has implemented. They are as follows:

1. National Intelligence Grid (NATGRID) - A central surveillance tool, it gives agencies real-time access from diverse sources like tax, banking, insurance, and travel to track threats effectively.
2. Central Monitoring System (CMS) - This enables agencies to directly tap into communications without telecom intermediaries, streamlining surveillance operations.
3. Network Traffic Analysis (NETRA) - It scans digital communication and analyses text across emails, social media and encrypted messages to detect potential threats online.
4. Automated Facial Recognition System (AFRS) - Mainly used by the Delhi Police, helps them identify and track individuals by comparing new images with the facial database.
5. Crime and Criminal Tracking Network System (CCTNS) - Designed to unify crime records, connects police stations and state units for better coordination.

These are the types of surveillance that the state has implemented to understand the threats our nation might face and to prevent them from causing harm.

In contrast to the extensive surveillance enforced by the state, the public has a contradictory

[34] 'Foucault's Surveillance State' (Number Analytics) https://numberanalytics.com/blog/foucaults-surveillance-state accessed 28 August 2025.

ISSN: 2582-6433

opinion. They opine that the state can never adopt any law that will work for the welfare of the state. They argue that there is are high chance that the government might misuse them for their benefit. In today's modern world, where everyone shares their intricate data with the government, like their address, Aadhaar card, BPL cards and ration cards and with the increase in UPI for payments, these can be used against us.[36] The police can use this to blackmail the citizens, it can also be used to spy on citizens or unfairly target them instead of using the data to protect them. Although there is a lack of concrete evidence, it can be gathered from news reports that Chandra Shekhar, India's ex-PM, claimed the V.P. Singh Government was involved in tapping twenty-seven politicians' phones and took the matter to the authorities. Moreover, it was also found that ex-PM Rajiv Gandhi's government was likely involved in the tapping of not only their ministers but also a large number of opposition members. The main issue that arises from all the above problems is that, in such a democratic country, the state government has used its own citizens' information against them illegally, causing a strained relationship between the netizens and the administration of the country. While all the surveillance is needed to protect the citizens, it is also imperative to maintain a balance between "security" and "privacy".

The judicial system should be held accountable too, in addition to the executive's failure. If there is a breach in privacy, only then will the judiciary step up, and even then, usually by chance, because most of the time, people won't even be aware that they are being spied upon.[37] The courts take a lot of time, with a lack in speedy trials for privacy cases and are immensely costly. The Radia Tapes scandal exposed the challenges that India faces with privacy. [38]Here, the controversy started when the Income Tax Department began to tap the corporate lobbyist Niira Radia's telephone conversations, accusing her of tax evasion and leaking over 5,800 conversations.[39] This reveals how the power of surveillance can even help citizens by exposing

[36] Abhijith Balakrishnan, 'Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards' (Express Computer, 2023) https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140 accessed 12 August 2025.
[37] Cyril Amarchand Mangaldas, 'Role of State Governments in India's Data Protection Regime' (Cyril Amarchand Mangaldas, March 2025) https://corporate.cyrilamarchandblogs.com/2025/03/role-of-state-governments-in-indias-data-protection-regime/ accessed 16 August 2025.
[38] Harish Salve, 'Niira Radia tapes leaked due to corporate rivalry: Ratan Tata to Supreme Court' Indian Express (New Delhi, 5 August 2023) https://indianexpress.com/article/business/business-others/niira-radia-tapes-leaked-due-to-corporate-rivalry-ratan-tata-to-supreme-court/ accessed 16 August 2025.
[39] JPC on Radia tapes?' India Today (New Delhi, 22 November 2010) https://www.indiatoday.in/india/story/jpc-on-radia-tapes-86005-2010-11-22 accessed 16 August 2025.

ISSN: 2582-6433

corruption, but it goes against privacy by recording private conversations. [40] Other instances of invasion of privacy by the state can be the use of government apps such as the DigiYatra app, the DigiLocker for students and other documents like Aadhar which contain sensitive personal information and details of an individual which can be accessed by the government anytime and anywhere without notifying the individual that their data has been intercepted for any official purposes.[41] There were also contentions by various notable political figures that the mass data collected through the app, and violated the established data security protocols. Such contemporary ongoing issues raise serious questions about the protection of privacy of an individual widening the mistrust of citizens with their personal information to the state. [42]

Although India has improved a lot with its data protection acts, such as the IT Act, 2000,[43] the Indian Telegraph Act, 1885 and the Digital Personal Data Protection Act,2023, it needs more insightful changes to curb future challenges in technology. There is a need for more independent tribunals in every state and not just the capital of the country (Digital Protection Board).[44] State surveillance should be during reasonable circumstances, and all data should be deleted once it is no longer needed.[45] For instance, various drones with webcams are sometimes used for tracking purposes, but the usage is unclear, and most of the time, the people are not even aware of this, violating their rules of natural justice. Hence, it is vital to bring changes in the existing laws to maintain a balance between government surveillance and individual security. As time evolves, with more technological advancements, safeguarding private information should be the utmost priority.

The term “Consensus” in the context of the issue between state surveillance and data privacy is not just about the legal harmonisation, but a balance between individual privacy rights and

[40] Harish Salve, ‘Niira Radia tapes leaked due to corporate rivalry: Ratan Tata to Supreme Court’ Indian Express (New Delhi, 5 August 2023) https://indianexpress.com/article/business/business-others/niira-radia-tapes-leaked-due-to-corporate-rivalry-ratan-tata-to-supreme-court/ accessed 19 August 2025.
[41] Disha Verma, 'Digi Yatra: Service or Surveillance?' The India Forum (online, 2025) https://www.theindiaforum.in/technology/digi-yatra-service-or-surveillance accessed 17 August 2025.
[42] Author unknown, 'Digiyatra Scandal Exposes Massive Data Breach' The Hindustan Gazette (online, 2025) https://thehindustangazette.com/latest-news/digiyatra-scandal-exposes-massive-data-breach-26702 accessed 18 August 2025.
[43] Ibid (n 1).
[44] Aksietha, 'Surveillance in India and Its Privacy Challenges in the Digital Age: A Legal and Constitutional Analysis' (2025) 10 International Journal for Research Trends and Innovation 652 https://www.ijrti.org/papers/IJRTI250308.pdf accessed 08 August 2025.
[45] Anuj Sharma and Kausiki Pegu, ‘Digital Personal Data Protection Act 2023: Employers’ Guide’ (SCC Online, 11 November 2024) https://www.scconline.com/blog/post/2024/11/11/digital-personal-data-protection-act/ accessed 11 August 2025.

ISSN: 2582-6433

the interests of the country. To sum up, data privacy in a sentence can be put as "The right of individuals to control their personal information". But then, is that possible, taking into consideration the current technological advancements? The need of the hour states there is a necessity to ensure that there is a check on the data utility, despite there being a clear violation of privacy, holding the security of the data as the topmost priority, which cannot be compromised. However, the clash between data privacy and state surveillance arises from the fact that the current surveillance system might violate the privacy of individuals and lead to a phenomenon of self-censorship, wherein individuals do not express their opinion freely, with the fear of negative consequences, which hinders the functioning of a democratic nation in a broader perspective.

The tussle between data privacy and Surveillance is not a very recent one. The have been various precedents that have evolved through history that portray the long-standing battle between the two. A remarkable case in the history of Privacy is the *People's Union of Civil Liberties (PUCL) vs Union of India*,[46] which was decided in the year 1997. In this particular case, the petitioner questioned the constitutionality of Section 5(2) of the Indian Telegraph Act, 1885,[47] which allowed the Government of centre or the State Government to intercept messages in a situation of public emergencies, believing it to be necessity for the protection of the sovereignty of the country, public order or for maintaining friendly relations with other nations. It was contended by the petitioner that this provision violated the Right to Privacy of an individual, highlighting the report by the Central Bureau of Investigations on the "Tapping of Politicians' Phones", which disclosed the procedural inadequacies in the phone tapping conducted by the Mahanagar Telephone Nigam Limited (MTNL) on the order of government officials. The Honourable Supreme Court, after all examination of facts, stated that the authorised government officer had to reasonably believe that the interception of messages was "necessary" in the interest of specific grounds:

1. Sovereignty and integrity of India
2. Security of the State
3. Friendly relations with foreign states
4. Public Order

[46] https://docs.manupatra.in/newsline/articles/Upload/E90FA90F-0328-49F2-B03F-B9FBA473964F.pdf accessed 19 August 2025.
[47] Indian Telegraph Act 1885 (India) s 5 https://indiacode.nic.in/handle/123456789/14917#section-5 accessed 24 August 2025.

ISSN: 2582-6433

5. Prevention of incitement to commit an offence.

Further, it was clarified that the officer could issue an order after a written recording of his/her statement. Though the provision was not declared unconstitutional, the court provided for a limit on the unreasonable powers of the state. In the landmark judgement of Justice K.S. Puttaswamy Vs Union of India[48], it was unanimously held by the nine-judge bench of the Honourable Supreme Court of India that "privacy" is to be constitutionally protected, as a facet of liberty, dignity and individual autonomy and that the Right of Privacy is a Fundamental Right. The honourable court applied the *Doctrine of Proportionality* and clarified that whenever a challenge is laid out against the state on the grounds of infringement of Right to Privacy, certain parameters have to be tested, and the state must prove that such infringement was a matter of necessity in the said circumstances, and the inability by the state to do so, will contend the claim of infringement of individual as legitimate.

In the International scenario, the case of *Big Brother Watch Vs the United Kingdom[49]* is a notable case, wherein the applicants pleaded before the European Court of Human Rights (ECTCHR) that the UK Intelligence Service had obtained mass data from underwater cables (bearers) through different surveillance techniques, which violated their right to respect for private life under *Article 8* of the European Convention on Human Rights[50], which respectively states that:

Article 8: Right to respect for private and family life*: "1 Everyone has the right to respect for his private and family life, his home and his correspondence.*

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The applicant further argued that fear of the interception, storage and exploitation of the communication might interfere with the journalist's rights of freedom of expression, which

[48] (Justice K. S. Puttaswamy - Digital Supreme Court reports) <https://digiscr.sci.gov.in/view_judgment?id=NjEwMg%3D%3D> accessed 21 August 2025.

[49] Big Brother Watch and Others v United Kingdom App nos 58170/13, 62322/14, 24960/15 (Grand Chamber, ECtHR, 25 May 2021).

[50] Equality and Human Rights Commission, 'Article 8: Respect for your private and family life' https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life accessed 25 August 2025.

ISSN: 2582-6433

violates *Article 10* of the European Convention on Human Rights,[51] which contends that:

Article 10: Freedom of expression: *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

Considering all the key points argued by the applicants, the European Court of Human Rights held that the regime was in violation of the said articles, and issued certain changes to be made to the provisions that are related to the aforementioned laws.

In view of other precedents and similar cases, we can come to the conclusion that bridging the wedge created between state surveillance and data privacy is nearly impossible. Nevertheless, there can be certain measures taken to create a sense of transparency in the system so that individuals can be assured that their data is not being misused or in unsafe hands. A few measures that can be implemented are:

1. Strengthening the Legal and Ethical Framework:

   The current framework for exploitation of the details, though, is certainly present, is not very clear. The requirements for any government organisation to collect information from various people should be made stricter, also the repercussions for misusing data or collecting unauthorised information should be severe, which creates a fear in the minds of criminals before committing a crime.

2. Technological and Policy Solutions:

   Techniques like data anonymisation can reduce the privacy concerns, at the same time allowing data use for security reasons. The idea of independent oversight and clear legal

[51] Equality and Human Rights Commission, 'Article 10: Freedom of expression' https://www.equalityhumanrights.com/human-rights/human-rights-act/article-10-freedom-expression accessed 24 August 2025.

ISSN: 2582-6433

boundaries should be encouraged, and the necessary changes have to be implemented. Embedding privacy protections is another measure that can be used, though at the outset it does not entirely guarantee privacy; harm can be minimised at best.

3. Contextual and Adaptive Approaches:

   Privacy regulations can be adapted to the context of data use, pertaining to certain situations, while maintaining a clear balance between the need for surveillance and safeguarding the privacy protections for individuals. Transparency regarding the surveillance practices that involve citizens can create more transparency and increase acceptance and legitimacy.

To summarise, in the current state of events, there is a huge divergence between data privacy and state surveillance. To put it lightly, it is very clear that they don't go well together. Henceforth, to improve the situation, the state has to clearly take steps towards better transparency and make certain changes in correspondence with the newly emerging technological evolution in the current legislation to gain the trust of citizens with their private information, which might lead to a better acceptance among society with respect to data privacy laws. Given the speed at which the current technology sector is growing, the state has to realise that there is a clear need to make changes regularly in this specific domain, especially when it is a subject of clear sensitivity among citizens and can highly disrupt the smooth functioning of a country, even in cases of very minimal errors.[52]

VI. COMPARATIVE STUDY BETWEEN INDIA, CHINA AND SINGAPORE

The growth of digital economies has created a surge in the need for protection of personal data and privacy concerns. The scope of government surveillance has become a major legal and policy concern. Asia, specifically, has seen a major acceleration in digital infrastructure from the late 1990s and early 2000s, with the emergence of e-commerce platforms, digital payment systems and various other technologies. Two of the leading nations in Asia, China and Singapore, have built unique security systems, regulating data privacy in two different approaches.

On one hand, Singapore has a Personal Data Protection Act, 2013(henceforth referred to as

[52] R Aksietha, 'Surveillance in India and Its Privacy Challenges in the Digital Age: A Legal and Constitutional Analysis' (2025) 10(3) International Journal for Research Trends and Innovation 651.

ISSN: 2582-6433

'PDPA'), which focuses on safeguarding the personal data of individuals from any misuse and maintaining a balance between the needs of organisations to collect, use or disclose personal information for legitimate purposes.[53] The Personal Data Protection Commission (PDPC) is empowered to enforce the PDPA regulations. On breach of any PDPA provisions, the PDPC is issued powers to stop the person from collecting, using or disclosing personal data, destroy the data which has been collected in contravention of the Act, or pay a financial penalty as compensation. [54]The Data Protection Appeal Panel is an independent body that hears appeals against the decisions of the PDPC, based on the provisions provided in the PDPA. In short, Singapore's PDPA is crafted in a manner that encourages the growth of data innovation, all the same while prioritising responsible data usage and trust in Singapore as a global data hub. The fundamental drawback in the legislation is the narrow application of laws mainly to the private sector organisations, which creates a leeway for the governmental agencies. Also, limited judicial remedies are another major issue that pertains to the Singapore legislation.

On the other hand, the primary laws which govern China's data privacy are Personal Information Protection Law (PIPL, 2021), the Data Security Law (DSL, 2021) and the Cybersecurity Law (CSL, 2017).[55] These operate together with the 'Three Key Regulations', which are:

1. The Regulations for the Administration of Network Data Security (RANDS)
2. The Security Protection Regulations for Critical Information Infrastructure and
3. The Regulations on the Graded Protection for Cybersecurity

PIPL maintains a stark similarity to other data protection laws in the world; in contrast, the DSL is a more nationally driven, public interest-inflicted law that focuses on preventing harm to the nation through data-enabled means. The major setback of the Chinese regulations is the excessive state control over the laws and their rigid cross-border mechanism, which leads to limited public transparency and international implementation challenges and complexities. [56] China has three primary laws that govern data privacy and state control, namely the PIPL, DSL

[53] Personal Data Protection Act 2012 (Singapore) https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act accessed 30 August 2025.
[54] Personal Data Protection Commission Singapore, 'Homepage' https://www.pdpc.gov.sg/ accessed 29 August 2025.
[55] Aho B and Duffield R, 'Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China' (Latest TOC RSS, 2 April 2020) <https://www.ingentaconnect.com/content/routledg/reso/2020/00000049/00000002/art00001> accessed 31 August 2025.
[56] Bird & Bird, 'China data protection and cybersecurity: Annual review of 2024 and outlook for 2025' (Insights, 2025) https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii) accessed 29 August 2025.

ISSN: 2582-6433

and CSl. However, their major issue is that, despite having so many laws, the state has wider power to control their data and access it. This creates a conflict between their personal rights and state control.[57] For instance, facial recognition is given huge importance to monitor the citizens' actions. China's laws are stricter than the EU's GDPR and mention higher requirements than those. In contrast, Singapore has a long-established legislation, the PDPA, which is more pragmatic and business-friendly. Even so, being a technological and financial hub, they face challenges regarding maintaining a balance between keeping people's privacy and encouraging innovations. Singapore's laws are, in comparison, less stringent than China's and are almost in par with the EU's GDPR. Whereas India has an entirely new law, which has just begun its journey in 2023, the DPDPA. India is still navigating how to put this law into use, as the implementation is rigid, with very little data literacy around the nation. The law exempts the government from certain actions and has many gaps in enforcing the law, raising concerns about fairness. On the other hand, China prioritises government control. This has resulted in people becoming more conscious of their digital footprints. The state's main goal is to expand state power, leading to distrust in digital systems and limiting freedom of expression. Conversely, Singapore has a high level of trust among its citizens and their business and their government. People are satisfied with the laws and are comfortable using them. Their law pushes business growth, and people are generally seen accepting data for security usage without even questioning it. [58]

To sum up, all three nations handle data privacy in their separate ways and are based on different grounds and priorities. While China is stricter and gives more power to the government, with its three laws (PIPL, DSL, and CSL), Singapore's law is more concentrated on increasing business growth and people trust their government; however, it is weaker when it comes to offering strong legal remedies to citizens regarding privacy. On the other hand, India's new DPDPA, 2023, is yet to be fully enforced in all the regions, especially in the rural areas.

[57] DLA Piper, 'Data protection laws in China' (DLA Piper Data Protection Laws of the World, 2025) https://www.dlapiperdataprotection.com/index.html?c=CN accessed 29 August 2025.
[58] Personal Data Protection (Notification of Data Breaches) Regulations 2021 (Singapore) https://sso.agc.gov.sg/SL/PDPA2012-S63-2021?DocDate=20210930 accessed 28 August 2025.

ISSN: 2582-6433

VII. CONCLUSION AND SUGGESTIONS

This article has so far traced how India, along with other Southeast Asian countries, has developed its data protection regulations in response to the growing digital era. The evolution of data protection laws in India demonstrates how rapidly digital technologies have modified our lives and how imperative it is for us to catch up to the laws. However, the disagreement between state surveillance and data protection has entered a critical phase, which creates an air of distrust and uncertainty between the two.[59] Even though the nations have taken several safeguarding steps to bring an equilibrium, the real task lies in making these protections effective and meaningful. The possible methods of curbing these problems are by firstly, building a reliable mechanism, like an independent data protection authority in every territorial area, to ensure accessibility across the country. Another mode of internet regulation is a self-regulation model, where the internet should be able to govern itself. Netizens have to ground themselves in certain communities, whereby they will have the same standards to follow.[60] It is believed to be the ultimate form of democracy. Additionally, a greater investment in digital literacy is required to make people aware, especially in rural areas. Data stored can also be used for research for security purposes without disclosing personal information. Along with that, whistleblowers should be encouraged to report any misuse of surveillance powers that the government possesses. Thus, a balanced digital future requires more than laws and theories. It demands transparency in surveillance and privacy-friendly technologies that can ensure accountability while safeguarding rights. By combining all the safeguards and active citizen participation, nations can achieve a fair balance between state security needs and individual data privacy, fostering both trust and security in the digital era.

[59] Press Information Bureau, Government of India, 'Progressive, Liberal and Contemporaneous: IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (PIB, 2021) https://www.pib.gov.in/PressReleasePage.aspx?PRID=1700766 accessed 28 August 2025.

[60] Ministry of Electronics and Information Technology, Government of India, Review of Legislations on Online Content Regulation in the World (May 2024) https://www.meity.gov.in/static/uploads/2024/05/Internship-Report-Review-of-Legislations.pdf accessed 2 September 2025.