FROM PUTTASWAMY TO DPDP 2023: CONTINUITY AND CONTRADICTIONS IN INDIA'S PRIVACY JURISPRUDENCE

Tamanna, LL.M., University Institute of Legal Studies, Chandigarh University

ABSTRACT

'K.S. Puttaswamy' where the Court held that privacy is a fundamental right. Union of India (2017) brought a statutory data protection regime in the country. The Digital Personal Data Protection Act, 2023 (DPDP Act) is formalization of this transformation as it converts the concept of privacy from being a vague constitutional principle to being a codified compendium of rights, duties and sanctions. This investigation traces the doctrinal development of the concept of privacy from the tentative judicial references in early cases, to the landmark Puttaswamy judgments to post 2017 jurisprudence that brings into the foreground of the right to privacy the principles of proportionality, necessity, and purpose limitation. It then examines the approach of the DPDP Act in operationalising these principles through its role-based definitions, the requirements of consent and notice, the rights of Data Principals and the creation of the Data Protection Board of India.

In addition, privacy has a direct relationship to criminal procedure and evidence. The Bharatiya Nagarik Suraksha Sanhita (BNSS) has the power to call for the discovery of digital evidence and the Bharatiya Sakshya Adhiniyam (BSA) lays down conditions pertaining to the admissibility and authenticity of electronic records. Bharatiya Nyaya Sanhita (BNS) penalises the violation of privacy such as voyeurism, stalking and impersonation. These statutes collectively illustrate both compatibilities and conflicts in the right to erasure could contradict with mandatory evidence preservation as well as in proportionality assessments being required to govern powers of investigatory action.

By way of a doctrinal analysis of the DPDP Act and its interrelation in BNSS, BSA, and BNS, this study attempts to show that Privacy in India has become a multi-layered concept - constitutional in genesis, statutory in structure, and procedural in application. It claims that the key challenge is to balance the character of those regimes to protect dignity and autonomy on the one hand,

and allow for legitimate governance, investigative and accountability functions in the digital age on the other.

Keywords: Data Principal, Data Fiduciary, Significant Data Fiduciary, BNSS, BSA, DPDP Act, 2023

1. INTRODUCTION

The transition from "*K.S. Puttaswamy v. Union of India*[1]" to the "Digital Personal Data Protection Act, 2023" reshapes privacy in India. It changes from a constitutional guarantee created by judges to a clear legal framework with rights, duties, and penalties. The focus shifts from rights to processing. The DPDP Act defines key players, establishes legal bases, provides detailed rights, and sets up a "Data Protection Board of India" for dispute resolution. The text of the Act outlines standards for consent, age restrictions for children, exemptions for certain government and legal actions, and different responsibilities for "Significant Data Fiduciaries." If you read carefully, you will see both continuity with Puttaswamy's ideas on dignity and autonomy and significant changes where ease for administration, state needs, or platform governance take priority. This creates conflicts with criminal procedure and evidence law. The "Bharatiya Nagarik Suraksha Sanhita" allows for searches, production, and warrants, while the "Bharatiya Sakshya Adhiniyam" outlines rules for admitting digital records. These intersections are where your research should focus.

After Puttaswamy declared that privacy is part of basic rights, India needed a general data protection law. The DPDP Act is that law. It outlines who you are in data relationships, the reasons that justify processing, and how you can respond to misuse. "Section 2 of the DPDP Act, 2023" defines "Data Principal," "Data Fiduciary," and the "Board," grounding the system in specific roles rather than vague ideas. "Sections 5 to 7" cover notice, consent, and some legitimate uses, while "Sections 11 to 13" establish rights to access, correction, erasure, and grievance resolution. "Section 10" allows the government to notify "Significant Data Fiduciaries," with additional requirements like Data Protection Impact Assessments and a Data Protection Officer based in India. "Chapter V" creates the "Data Protection Board of India" under "Section 18," turning privacy disputes into a specialized adjudication process. On the criminal and evidentiary side, the "BNSS" maintains powers to compel production and search through "Sections 94 and 96," while the "BSA" updates how electronic records are treated as

[1] (2017) 10 SCC 1

evidence through "Sections 61 to 66" and the "Schedule" certificate model. The "BNS" revises offences related to informational privacy, including "Section 77" on voyeurism and "Section 78" on stalking, which often intersect with digital harms. Together, these laws define your practical rights: a constitutional right filtered through broad data rules, enforced alongside strict criminal procedures and digital evidence standards.

2. RESEARCH OBJECTIVES

This article outlines where constitutional doctrine and the DPDP Act agree and where they differ. This way, you can make clear doctrinal arguments and policy suggestions in upcoming chapters.

- Identify how "Section 2" definitions reframe the Puttaswamy subject as "Data Principal."
- Examine whether "Sections 5 to 7" on notice, consent, and legitimate uses preserve meaningful, revocable choice.
- Assess if "Sections 11 to 13" rights realize informational self-determination in practice.
- Evaluate "Section 10" SDF duties and whether DPIAs internalize dignity and proportionality.
- Analyze "Section 18" Board design for independence, due process, and remedies.
- Reconcile DPDP rights with "BNSS Sections 94 and 96" on summons and search warrants.
- Test admissibility of DPDP - compliant evidence against "BSA Sections 61 to 63" and the certificate "Schedule."[2]
- Situate privacy - adjacent BNS offences like "Sections 77 and 78" within DPDP's processing paradigm.[3]

[2] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), available at: https://www.indiacode.nic.in/bitstream/ 123456789/20063/1/a2023-47.pdf (last visited on September 15, 2025).
[3] West Bengal LLROA: Comparative Table of IPC 1860 And BNS 2023 (PDF), available at: https://wbllroa.in/ wp-content/uploads/2024/07/COMPARATIVE-TABLE-OF-IPC-1860-BNS-2023-ADV-GURENDER RANA.pdf (last visited on September 16, 2025).

3. METHODOLOGY

A doctrinal analysis combines a close reading of the DPDP Act's text with checks in the "BNSS," "BSA," and "BNS." This method follows the internal logic of "Sections 2, 5–13, 10, and 18" of the DPDP Act. It also examines friction points with "BNSS Sections 94 and 96" and "BSA Sections 61–63," including the "Schedule" certificate. Limited comparative touchpoints provide context without overshadowing Indian materials. The case discussion focuses on framing rather than proof. All propositions depend on the statutory text from official sources.

4. CONSTITUTIONAL DEVELOPMENT

The privacy in India has evolved from occasional judicial hints to a clear constitutional guarantee. This guarantee now shapes lawmaking, oversight, and decision-making. In the early cases, judges discussed privacy as part of personal freedom under Articles 19 and 21. Later rulings recognized it as an independent fundamental right linked to Articles 14, 19, and 21. This change is significant because it creates the legal framework for later laws, such as the Digital Personal Data Protection Act, 2023. This act has a role-based structure in Section 2 and outlines rights and responsibilities in Sections 5 to 13. It also establishes standards for limitations, requiring proportionality and necessity as constitutional tests for any legal exemptions. These tests are supported by strict laws regarding procedural powers in the Bharatiya Nagarik Suraksha Sanhita for summons and searches, as well as in the rules for electronic evidence under the Bharatiya Sakshya Adhiniyam in Sections 61 to 63. Overall, constitutional privacy is no longer just a theoretical idea. It is a set of rules that govern how surveillance, data management, and evidence function, whether in front of the Data Protection

Board of India under Section 18 of the DPDP Act, 2023, or in courts applying the BSA and BNSS to digital records.[4]

4.1 PRE-PUTTASWAMY JURISPRUDENCE

The legal cases before 2017 contributed to the emergence of a clear right. In "*Kharak Singh v.*

[4] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on September 17, 2025).

State of Uttar Pradesh,[5]" the Supreme Court ruled that nighttime visits to homes violated personal liberty. However, it permitted other types of surveillance, meaning the idea of privacy was still evolving but was connected to dignity. In "*Gobind v. State of Madhya Pradesh,*[6]" the court acknowledged privacy interests under Article 21 and agreed that regulation could occur with proper safeguards. The case of "*People's Union for Civil Liberties v. Union of India*"[7] focused on phone tapping and stressed that legal processes and oversight are essential for any intrusion. Through these cases, the Court moved from discomfort with intrusive practices based on liberty to a conditional acceptance based on procedure and necessity. This change laid the foundation for a more explicit recognition of privacy. It also suggested a shift toward formal procedures, which we see today in the "BNSS" search warrant system related to "Section 96." This system highlights the importance of records and authorizations, along with the "BSA" on electronic records, which permits digital evidence if it meets the standards in "Sections 61 to 63."[8]

4.2 PUTTASWAMY I (2017)

Puttaswamy v. The Union of India[9] changed the legal landscape by declaring privacy a fundamental right connected to dignity and liberty. This protection covers Articles 14, 19, and 21. The judgment established a clear test for restrictions. It requires legality, a legitimate aim, a rational connection, and proportionality with a necessity component. This framework now guides the evaluation of any data rule or surveillance measure, including the DPDP Act, 2023. For example, Section 5 on notice and Section 7 on certain legitimate uses should be analyzed with a focus on minimal impairment and a clearly defined purpose.

The clarity provided by this ruling also connects with criminal procedure and evidence law. When the State uses BNSS powers for summons or search under provisions linked to Section

94 and Section 96, it must follow the proportionality discipline described in Puttaswamy. When digital material is presented, the BSA ensures that Section 61 treats electronic records as admissible. Section 63 addresses the method of proof, reinforcing the link between privacy

[5] AIR 1963 SC 1295
[6] (1975) 2 SCC 148
[7] (1997) 1 SCC 301
[8] Columbia Global Freedom of Expression: Singh v. Uttar Pradesh, available at: https://globalfreedomofexpression.columbia.edu/cases/singh-v-uttar-pradesh/ (last visited on September 18, 2025).
[9] Supra Note 1

respecting collection and courtroom reliability. The key shift in this judgment is moving away from ad hoc balancing to a rights-centered inquiry that statutes and agencies need to adopt. This includes the Data Protection Board of India, which is established under Section 18 for handling breaches and providing remedies.[10]

4.3 PUTTASWAMY II AADHAAR (2018)

K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India[11] applied proportionality to a national identity project and produced a mixed outcome that offers helpful insights. The Court recognized that unique identification had valid goals, such as providing targeted subsidies. It then evaluated whether the program was necessary and proportional by examining the statute's features. The Court upheld the program's main components while removing aspects that were too broad or risked function creep. The reasoning emphasized purpose limitation, data minimization, and safeguards against profiling. These principles are now reflected in the "DPDP Act, 2023" through "Sections 5 to 7," which address notice, consent, and specific legitimate uses, and in "Section 10," which designates "Significant Data Fiduciaries" that require Data Protection Impact Assessments and Data Protection Officers. The decision's careful adjustments create a model for examining both State schemes and private platforms. This encourages focused designs and clear oversight. This method aligns with the "BNSS" requirement that searches and production use lawful warrants or summons with specificity under "Section 96." It also matches the "BSA" requirement that electronic records must be demonstrated in structured ways under "Sections 61 to 63," ensuring evidential reliability while respecting privacy. The Aadhaar decision's selective removals define the constitutional space for data processing while still respecting individual autonomy.[12]

4.4 POST-PUTTASWAMY DEVELOPMENTS

After 2017, courts and tribunals dealt with privacy issues related to personal freedom and dignity in different areas, including messaging platforms, workplace surveillance, and targeted verification. They often ordered investigations or expert assessments when the facts demanded

[10] 2017 10 (SCC) 1
[11] 2019 1 (SCC) 1
[12] Beghar Foundation through its Secretary and Another v. Justice K. S. Puttaswamy (Retd.) and Others, Review Petition (Civil) No. .../2021, Diary No. 45777/2018, Judgment dated 11 January 2021, available at: https://api.sci.gov.in/supremecourt/2018/45777/45777_2018_5_1001_25344_Judgement_11-Jan-2021.pdf (last visited on September 19, 2025).

it. The Supreme Court's involvement in the spyware case, "*Manohar Lal Sharma v. Union of India*[15]," showed that vague national security claims cannot block scrutiny. It also indicated that independent technical investigations might be necessary to evaluate the legality and necessity of surveillance claims. These changes relate to legal frameworks. The "DPDP Act, 2023" focuses on the "Data Principal" in "Section 2," guarantees rights in "Sections 11 to 13," and requires notification of breaches and accountability according to constitutional fairness. The procedural powers under the "BNSS" regarding searches and production must be applied with attention to detail and proper record-keeping based on fairness. The "BSA" in "Sections 61 to 63" highlights the need for reliable proof of electronic records. The field now expects institutions to balance privacy with valid state objectives through careful design, verifiable safeguards, and well-founded decisions, rather than broad claims. This expectation also applies to administrative practices before the "Data Protection Board of India" under "Section 18," where legality, necessity, and fairness should be standard practices for assessing processing, safeguards, and remedial actions.[13]

5. LEGISLATIVE FRAMEWORK

The laws that follow "*K.S. Puttaswamy v. Union of India*[14]" turn constitutional privacy into a clear set of duties, procedures, and standards that you can use. The "Digital Personal Data Protection Act, 2023" defines your role as a "Data Principal." It governs how "Data Fiduciaries" manage personal data, recognizes consent and some non-consent reasons, sets out rights for access, correction, and erasure, and establishes the "Data Protection Board of India."

The "Bharatiya Sakshya Adhiniyam" updates the law of proof for the digital age by allowing electronic records as evidence and including a computer output certificate in a formal Schedule. The "Bharatiya Nagarik Suraksha Sanhita" includes guidelines for searches, the production of evidence, audio and video recordings of seizures, and cooperation across borders, emphasizing proportionality. The "Bharatiya Nyaya Sanhita" sets protections for privacy-related crimes such as identity disclosure, voyeurism, and stalking. It also connects with "Sections 66C and 66D of the Information Technology Act, 2000," which address digital identity theft and fraud through impersonation. Together, these laws provide you with the tools to define rights, ensure

[13] Columbia Global Freedom of Expression: Pegasus Order — Supreme Court of India (PDF), available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/10/pegasus-order-supreme-court-403008.pdf (last visited on September 19, 2025).
[14] Supra Note 1

compliance, and establish accountability for both private individuals and the government.

5.1 DPDP Act, 2023 Overview

The "DPDP Act, 2023" applies to the processing of digital personal data in India. It also extends to processing outside India when it is related to offering goods or services to individuals in India. "Section 3" states that the Act covers data collected in digital form or in non-digital form and then digitized, while stating certain exclusions. The Act follows a purpose-first and role based structure. It requires a lawful purpose and links processing to either consent or "certain legitimate uses." It assigns "Data Fiduciaries" specific duties and outlines additional responsibilities for "Significant Data Fiduciaries." It acknowledges your rights and explains how to file a complaint with the "Board." Reading "Sections 3 to 7" alongside the later chapters on rights and enforcement helps you understand the balance the law aims to strike between personal autonomy and administrative efficiency.

5.1.1 Consent and Notice

Consent under the DPDP Act, 2023 is specific, informed, and can be revoked. Section 5 requires a Data Fiduciary to provide a clear notice that outlines the personal data to be processed, the purpose of the processing, how you can exercise your rights, and how to file a complaint with the Board. Section 6 mandates that consent requests be in clear and simple language, with the option to access them in English or any language listed in the Eighth Schedule. It also acknowledges your right to withdraw consent as easily as you give it. Any attempt to bundle consent with the waiver of complaint rights will not work, as shown in the example. These clauses demand a design for consent flows that can be audited. This is crucial when assessing fairness against the constitutional standards of necessity and minimal impairment.

5.1.2 Certain Legitimate Uses

Section 7 of the DPDP Act, 2023 outlines non-consent grounds called "certain legitimate uses." These include situations where you voluntarily share personal data for a specific purpose, where processing is necessary for the government to carry out a legal function, or for reasons related to sovereignty and security. It also covers cases where processing is needed to fulfill other legal obligations. This provision highlights use cases, such as employment or benefits

delivery, that can happen without new consent, provided they follow the statute's rules. The legal wording requires careful attention to specifying purposes, documenting processes, and maintaining safeguards to ensure the use is suitable for its intended goal. For practitioners, this clause will form the legal foundation for many high-volume workflows in both public and private sectors, and it is where audit and accountability measures must be prioritized.

5.1.3 Children's Data

Section 9 of the DPDP Act, 2023, creates specific rules for children. It requires clear consent from a parent or legal guardian before handling a child's personal data and sets strict limits on practices that profile, track, or target ads at children. This provision demands a high standard of care, requiring both technical and organizational steps. These steps include age verification, reducing data collection, and managing content on platforms that children commonly use. Product teams must show how their defaults prevent behavioral tracking and targeted messaging to minors. Legal teams must ensure that notices and consent collection are clear and easy to understand for guardians. When combined with Section 10, which applies to entities labeled as Significant Data Fiduciaries, this clause expands the evaluation of governance and risk in services that have many child users.

5.1.4 Significant Data Fiduciary

Section 10 of the DPDP Act, 2023 gives the Central Government the authority to identify a Significant Data Fiduciary by evaluating factors like the amount and sensitivity of personal data, risks to the rights of Data Principals, and possible effects on sovereignty and public order. After identification, an SDF must appoint a Data Protection Officer based in India, hire an independent data auditor, and carry out regular Data Protection Impact Assessments. This section promotes privacy by design in management practices by requiring documented risk identification, mitigation, and independent oversight. For you, this means that larger or higher risk processors need to have clear governance, internal escalation procedures, and a duty to provide evidence of their fairness judgments. It also sets up a compliance gradient in the market, where this designation shows the level of privacy controls organizations are expected to have in their daily operations.

5.1.5 Data Principal Rights

The DPDP rights are useful tools. "Section 11" gives you the right to get a summary of your

personal data being processed and the activities related to it. “Section 12” allows for correction, completion, and erasure, depending on valid reasons for keeping the data. The law also creates a system for complaints that requires a “Data Fiduciary” or “Consent Manager” to reply within set timeframes. It introduces a nomination right in “Section 14.” Importantly, the text includes exceptions where State processing or legal duties can limit or delay the exercise of rights. “Section 12(3)” specifically restricts correction or erasure in certain State cases. When considered alongside “Section 13” about handling grievances, the rights chapter encourages data processors to keep accurate records, responsive platforms, and reliable deletion methods that can hold up under review and challenge.

5.1.6 Enforcement Framework

“Section 18 of the DPDP Act, 2023” establishes the “Data Protection Board of India” as a corporate body with a digital workflow. “Sections 19 to 22” cover the Board's composition, qualifications, and tenure. The chapter on powers and functions gives the Board the authority to investigate breaches, issue directions, accept voluntary commitments, and impose fines based on a statutory Schedule. The text outlines a tech-driven approach, allowing proceedings, notices, and orders to be entirely digital. It also states that penalties will consider the seriousness, duration, and mitigating actions involved. “Section 34” directs collected penalties to the Consolidated Fund of India. This change shifts privacy into a regulated compliance area with a structure for adjudication and opportunities for appeal to the Telecom Disputes Settlement and Appellate Tribunal. It also includes a clear non-derogation clause that outlines how conflicts with other laws will be handled in practice.

5.2 BSA 2023 and Electronic Evidence

The “Bharatiya Sakshya Adhiniyam, 2023” updates evidence for digital settings. It allows electronic records to be accepted as evidence and dismisses the idea that format alone can negate evidentiary value. It establishes a legal way to prove content using computer outputs that meet specific conditions. The law also creates assumptions about the integrity and authenticity of secure electronic records and signatures. This combined impact highlights the need for reliable logging, device integrity, and certificate practices for those involved in litigation and investigations. If your privacy-compliant system produces audit trails and certificates that match the requirements in the statute’s Schedule, those documents also serve as proof. This connects privacy protections and evidence laws in a very practical manner.

5.2.1 Electronic Records and Admissibility

"Section 61 of the Bharatiya Sakshya Adhiniyam" recognizes electronic records as admissible, following the guidelines in "Section 63." "Section 62" states that contents can be proved according to "Section 63." "Section 63" outlines the full computer output rule with conditions that include regular use, ordinary course input, proper operation, and accurate reproduction. It requires a certificate that identifies the record, explains how it was created, describes the device used, and addresses those conditions. The statute includes a Schedule certificate format that must accompany the electronic record whenever it is submitted. This need for repeatable, documented proof means your systems should create exportable, signed logs with device details and chain of custody information to avoid future challenges about authenticity or changes.

5.2.2 Presumptions for E Records and e Signatures

Section 85 of the Bharatiya Sakshya Adhiniyam tells the court to assume that every electronic record claiming to be an agreement with electronic or digital signatures was created using those signatures. Section 86 builds on this by setting assumptions for secure electronic records and secure electronic signatures. This includes an assumption that there were no changes made since the time related to the secure status and an assumption that a secure electronic signature was added with the intent to sign or approve the record. These assumptions help ensure the integrity and authorship of records. They also highlight the importance of cryptographic controls and standards that qualify a record as secure. This change in the burden of proof can impact disputes over authenticity right from the beginning.

5.3 BNSS 2023 and Procedure

The "Bharatiya Nagarik Suraksha Sanhita, 2023" outlines procedures for the digital age. "Section 94" allows for summons that require the production of documents or items. This includes electronic communications and devices that may hold digital evidence. "Section 96" establishes the rules for issuing search warrants. It allows for general searches when justified. "Section 105" mandates that searches and seizures be recorded with audio and video technology. These provisions guide investigative practices toward methods that are documented, reviewable, and supported by technology. For your privacy analysis, these powers must be used carefully and specifically. Their results must meet the evidentiary standards set

by the "BSA." Clear safeguards, precise descriptions of the data being sought, and audio-visual recordings of warrant executions are practical ways to ensure that these powers fit the principles of proportionality defined in "Puttaswamy."[15]

5.3.1 BNS 2023 Privacy Protective Offences

The "Bharatiya Nyaya Sanhita, 2023" includes several offenses related to privacy and online behavior. It bans revealing identities in sensitive situations and punishes voyeuristic capture and sharing of private acts. Stalking is also illegal, which covers persistent electronic monitoring and unwanted contact. The code defines cheating by impersonation and shows how impersonation can harm people online. Therefore, it should be read alongside "Sections 66C and 66D of the Information Technology Act, 2000," which focus on identity theft and cheating by impersonation using a computer resource. When you look at these offenses together with the DPDP processing rules and the BNSS procedures, you see a layered model. In this model, wrongful collection, misuse, and abusive sharing of personal data can lead to regulatory action and criminal penalties.

5.3.2 Disclosure of Victim Identity

Section 72 of the Bharatiya Nyaya Sanhita prohibits printing or publishing the name or any information that could reveal the identity of someone accused of certain sexual offenses. There are a few exceptions, like when the victim or their next of kin gives written permission in specific situations. This rule is important for how newsrooms operate, social media discussions occur, and content is managed on various platforms. If you run a platform or manage content, you need filters and policies that can identify and block text or images that might reveal identities in violation of this section. When used with the notice and purpose limits of the DPDP Act, 2023, organizations can show they care about how they handle and publish information. This approach helps protect survivors and lowers legal risks.

5.3.3 Voyeurism

The "Voyeurism" in the "Bharatiya Nyaya Sanhita" corresponds to "Section 76." This section punishes anyone who captures images of a woman involved in a private act without her consent

[15] PRS Legislative Research: Bharatiya Nagarik Suraksha Sanhita, 2023 (PDF), available at: https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nagarik_Suraksha_Sanhita%2C_2023.pdf (last visited on September 20, 2025).

and then publishes or shares that material. The law specifically targets unauthorized visual capture and the distribution of such images, including online sharing. For your compliance plan, this requires actively detecting the sharing of intimate images, establishing strict takedown standards, and setting up cooperation with law enforcement that follows the "BNSS" requirements and the "BSA" proof rules. It also relates to the "DPDP Act, 2023," which addresses children's data and profiling limits. The same technical tools used for targeted ads can also be used to stop the spread of sensitive intimate content. This illustrates how privacy engineering can support both regulatory and legal compliance.[16]

5.3.4 Stalking Including Online Monitoring

"Section 77 of the Bharatiya Nyaya Sanhita" addresses stalking by defining actions like following a woman, repeatedly trying to engage when she shows clear disinterest, and tracking her use of electronic communication. Including electronic monitoring fills a crucial gap in previous practices. It recognizes that privacy harms can occur through device tracking, constant messaging, and monitoring online status or location. For your policy stack, this means setting rules at the workplace and platform levels that ban repeated contact after consent is withdrawn. It also involves creating block and report functions that produce logs compliant with "BSA." Additionally, it requires working with "BNSS" orders for device or account information. Furthermore, it encourages platforms to perform Data Protection Impact Assessments under "Section 10 of the DPDP Act, 2023" to prevent features from being misused for harassment.[21]

5.3.5 Cheating by Personation Online

Cheating by personation is defined in "Section 317 of the Bharatiya Nyaya Sanhita." This section outlines the offense and the punishment for pretending to be someone else or swapping one person for another. In an online context, this relates to "Section 66C of the Information Technology Act, 2000," which deals with identity theft, and "Section 66D of the Information Technology Act, 2000," which focuses on cheating by personation through a computer resource. Together, these clauses address fake profile fraud, credential theft, and impersonation scams on email, messaging, and social media platforms. Your prevention and response program should include identity verification, anomaly detection, and evidentiary logging. This should meet the requirements of the "BSA" certificate regime. The legal basis for processing these

[16] Bharatiya Nyaya Sanhita, 2023 (PDF), available at: https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita%2C_2023.pdf (last visited on September 20, 2025).

signals typically falls under "Section 7 of the DPDP Act, 2023," as it counts as a legitimate use for preventing fraud and complying with the law.

6. CONTINUITIES AND CONTRADICTIONS

To trace the shift from viewing privacy as a constitutional guarantee to seeing it as a managed processing framework by comparing "*K.S. Puttaswamy v. Union of India*" with the "Digital Personal Data Protection Act, 2023." The DPDP Act creates a role-based system in "Section 2." It outlines its scope and reach beyond Indian borders in "Section 3." It also divides lawful processing into consent in "Sections 5 and 6" and "certain legitimate uses" in "Section 7." The law establishes rights in "Sections 11 and 12" and sets up the "Data Protection Board of India" in "Section 18." Your constitutional perspective is still important because State pressure and evidence use connect with the "Bharatiya Nagarik Suraksha Sanhita" in "Sections 94, 96, and 105" and the "Bharatiya Sakshya Adhiniyam" in "Sections 61, 62, 63, 85, and 86." The resulting connection is not perfect. It is a dynamic relationship where consent, proportionality, procedure, and proof need to interact effectively in practice across various platforms, agencies, and courts.

7. CONSTITUTIONAL PRINCIPLES CARRIED FORWARD

To see a clear connection in the DPDP Act, which focuses on consent, dignity, and control. "Section 5" requires a clear notice that outlines purposes, data categories, rights pathways, and complaint options before any processing starts. "Section 6" insists on consent that is specific, informed, and easy to withdraw. "Section 9" protects children by requiring verified guardian consent and by limiting profiling, tracking, and targeted ads aimed at them. These sections put human choice into system design and take a child-first approach that reflects the constitutional emphasis on vulnerability and harm prevention. The move from words to rules shows clearly in the details. The consent request must use simple language. The pathway for withdrawal cannot be complicated. The example in the Gazette clearly states that you cannot bundle consent with giving up the right to approach the Board. These aspects make autonomy tangible in forms, screens, and logs that you can review.

7.1 Proportionality vs Statutory Bases

While examining "Section 7" on "certain legitimate uses" to see if non-consent processing

meets the constitutional requirement for necessity and least restrictive means. The list is extensive. It includes voluntary provision for a specific purpose, compliance with the law, and state functions related to sovereignty, security, and benefits delivery. It also covers employment and reasonable purposes that align with the text. The connection to proportionality depends on how clearly a purpose is defined, how narrowly data is limited, and how effectively safeguards minimize collateral impact. Documentation is crucial. A processor must show that a notice outlined the task, that the data collected was the minimum needed, and that retention matched the purpose's lifecycle. Internal records, role-based access, and proof of deletion become the actual measure of necessity in practice. The law provides the foundation, but your logs and controls create the least restrictive means narrative when challenged.

7.2 State Processing and Exemptions

The strongest tension in State-facing clauses and notification-based relaxations next to the constitutional promise of strict scrutiny for intrusive action. “Section 7” allows processing for State functions and security purposes. “Section 10” gives the government the power to notify “Significant Data Fiduciaries,” set additional duties, and adjust oversight for high-risk actors. These tools can improve accountability in large public systems; however, they can also create an imbalance where the State has broader legal grounds than private actors. The solution depends on how officials define necessity, ensure purpose limitation, and publish safeguards. On the procedural side, coercive access must still adhere to “BNSS Section 94” for summons, “BNSS Section 96” for warrants, and “BNSS Section 105” for recording audio and video during searches and seizures. These steps translate the proportionality requirement into warrants that explain what is being sought, why it is needed, and how the execution will be documented. The paperwork is not just for show; it forms the connection between legal permission and constitutional limits.

7.3 Rights Design and Limits

One exercise your rights through "Section 11" for access and "Section 12" for correction, completion, and erasure. "Section 13" creates a grievance process, while "Section 14" allows for nominations. These options show your control in a practical way, but they come with clear limits. Other laws may require retention, or ongoing State functions might be influenced. The setup asks you to consider your wish for deletion alongside legal responsibilities or ongoing actions. The main point is the quality of the process. A rights request should lead to identity

verification, determine the scope, and include system searches in both live and archived stores. It should also provide a clear response that explains the reasoning behind any action or refusal.

If refusal is due to a law enforcement exception, the processor must document the legal reason, the date range, and a plan for reviewing the issue when the proceeding concludes. This practice makes the limits clear and measurable, ensuring that the legal balance matches what the Constitution requires.

7.4 Evidence and Enforcement Interface

To test how privacy measures affect investigative effectiveness at the proof stage, we look at where the "Bharatiya Sakshya Adhiniyam" and the "BNSS" intersect with the DPDP scheme. "Section 61 of the BSA" says that electronic records are admissible. "Section 62" and "Section 63" explain the computer output and certificate system, using a Schedule format that ensures integrity and regular use. "Section 85" and "Section 86" provide presumptions for electronic records and secure electronic signatures, shifting the initial burden when cryptographic standards are met. On the procedural side, "BNSS Section 94" and "Section 96" outline production and warrants, while "Section 105" mandates audio and video recording of search and seizure. When we connect these elements, a collection that respects privacy does not weaken proof; it actually strengthens it. Narrow warrants help reduce irrelevant information. Proper logging keeps the chain of custody intact. Certificates turn audit trails into evidence that is ready for court. This method remains the best way to balance constitutional privacy with effective investigation in your daily cases.[17]

8. COMPARATIVE AND INTERNATIONAL PERSPECTIVES

When you compare India's scheme from "Section 2" to "Section 18 of the Digital Personal Data Protection Act, 2023" with leading global templates, you notice clear similarities in key safeguards. There is also a distinct choice regarding State interests and cross-border controls. The DPDP Act bases processing on consent in "Sections 5 and 6." It acknowledges non-consent grounds in "Section 7," establishes protections for children in "Section 9," increases obligations for "Significant Data Fiduciaries" in "Section 10," grants rights in "Sections 11 and 12," and establishes the "Data Protection Board of India" in "Section 18." This structure exists

[17] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), available at: https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on September 21, 2025).

alongside procedural and evidentiary laws that influence enforcement and proof.

The global examples most often mentioned in Indian discussions are the EU's GDPR, the UK GDPR, Singapore's PDPA, South Africa's POPIA, and Brazil's LGPD. These laws combine strong rights with risk-based compliance, set timelines for breach notifications, and provide

organized rules for international transfers. The goal is to evaluate the DPDP Act's focus on consent and its notification-based cross-border model against the established practices of these other regimes. This allows for an assessment of alignment with constitutional privacy and points of conflict that might need careful rulemaking.

8.1 EU GDPR Contrast

The EU GDPR offers several legal bases beyond consent in Article 6. It sets a higher standard for special categories in Article 9. Independence of regulators is established in Article 52, which requires supervisory authorities to act independently and stay free from outside influence. A systematic risk analysis is mandatory under Article 35 for Data Protection Impact Assessments. Furthermore, breach notifications to the supervisory authority must happen without unnecessary delay and, when possible, within 72 hours as outlined in Article 33. These rules work within a one-stop shop enforced by independent authorities, as described in Articles 57 to 58. This creates a strong culture of compliance focused on risk and accountability. In India, Section 10 references DPIA-style thinking for Significant Data Fiduciaries. However, the EU approach makes DPIAs standard for certain high-risk processing and links breach timing to a clear 72-hour deadline. In contrast, India's upcoming rules are likely to implement breach notices through the Board's digital procedures instead of a specific statutory time frame. Transfers in the EU depend on Article 45 adequacy, Article 46 safeguards, and Article 49 exceptions, forming a layered structure for permissibility.[18]

8.2 UK and Singapore

Post Brexit, the UK GDPR keeps the structure of the GDPR but adds local changes through the "Data Protection Act 2018." The Information Commissioner's Office guides businesses on risk-based duties, offering strong advice on DPIAs and breach reporting. You must assess high

[18] EUR-Lex: General Data Protection Regulation (EU) 2016/679 (English), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (last visited on September 22, 2025).

risk processing before launching and report any significant breaches to the ICO within 72 hours. This timeline is similar to the EU's rules. The UK's transfer options include adequacy decisions and the International Data Transfer Agreement for cases where adequacy is not available. Singapore's PDPA provides a different but useful approach. Every organization names a "Data Protection Officer" according to "Section 11." It encourages compliance with guidance from detailed PDPC advisories. Since the 2020 updates, it also recognizes a "legitimate interests" exception, which comes with documented assessments and mitigation responsibilities. Singapore requires organizations to notify the PDPC of data breaches within three calendar days and inform individuals promptly if there is a risk of significant harm or if the breach affects a large number of people.

This blend of legal obligations and guidance from regulators has created a practical, risk-based culture. India can learn from this while setting up "Section 10" governance rules and breach procedures for Boards as stated in "Section 18."[19]

8.3 Emerging Democracies

Among emerging democracies, South Africa's "Protection of Personal Information Act" emphasizes rights and limits on purpose. It mandates notifying both the Information Regulator and affected individuals in case of a security breach under "Section 22," along with guidance materials that clarify what information to share. Brazil's "Lei Geral de Proteção de Dados" has a structure similar to the GDPR, featuring multiple legal bases, strong rights, and a powerful national authority, the ANPD. The ANPD offers official publications that include consolidated English translations and operational guidance. Latin American countries often combine rights heavy texts with formal oversight. Argentina's "Law 25,326" is an early example, featuring registration and transparency duties monitored by the AAIP. At the same time, Mexico's updated private sector law still relies on privacy notices and specified legal bases and is undergoing reforms related to data transfers and supervision. These systems show that strong oversight and clear breach protocols can lead to consistent enforcement without hindering economic activity. They also highlight the importance of templates and checklists from regulators, which can assist small controllers. India's Board may adopt similar methods through digital processes described in "Section 18," while ensuring compliance with rights in

[19] Information Commissioner's Office (UK): Guide to Law Enforcement Processing — Personal Data Breaches, available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/personal-data breaches/ (last visited on September 22, 2025).

"Sections 11 and 12" and high-risk governance in "Section 10."[20]

8.4 International Data Flows

International data flows are the clearest comparison. The EU system favors adequacy through "Article 45 GDPR." This allows free transfers when the Commission finds protection that is basically equal. Otherwise, it uses "Article 46" safeguards like Standard Contractual Clauses and "Article 49" exceptions for remaining cases. The UK follows a similar path with UK adequacy and domestic transfer tools, ensuring business certainty through consistent guidance. India's cross-border model in "Section 16 of the DPDP Act, 2023" takes a notification-based or "negative list" approach. Transfers are generally allowed unless the Central Government restricts specific countries or territories through notification. There may also be sector-specific exceptions. The practical result is less friction for global processing along with sovereign control to limit destinations where protection is not sufficient. Draft and tertiary documents explain the criteria the Government may consider. They also outline how organizations can meet contractually and technically while waiting for specific notifications. For your compliance map, this means creating a baseline control set that can handle any transfer. Keep records to support "Sections 5 to 7" purposes and "Section 10" governance. Stay alert for notified restrictions that could require changes in routing or additional safeguards similar to adequacy assessments in other regions.[21]

9. CHALLENGES AND THE WAY FORWARD

The connection from "*K.S. Puttaswamy v. Union of India*[33]" to the "Digital Personal Data Protection Act, 2023" relies on the choices made by regulators, fiduciaries, and courts in their daily work. Your goal is to uphold dignity and autonomy within consent flows, audit logs, and warrants instead of treating them as mere slogans. The DPDP Act outlines definitions in "Section 2," its scope in "Section 3," consent and notice in "Sections 5 and 6," non-consent bases in "Section 7," protections for children in "Section 9," obligations for "Significant Data Fiduciaries" in "Section 10," rights in "Sections 11 and 12," and an enforcement forum in

[20] Information Regulator (South Africa): Guidelines on Completing a Security Compromise Notification (Section 22 POPIA) (PDF), available at: https://inforegulator.org.za/wp-content/uploads/2020/07/Guidelines-on completing-a-Security-Compromise-Notification-ito-Section-22-POPIA.pdf (last visited on September 23, 2025)

[21] GDPR-Info: Article 45 — Transfers on The Basis of An Adequacy Decision, available at: https://gdpr-info.eu/art-45-gdpr/ (last visited on September 23, 2025

"Section 18." The "Bharatiya Nagarik Suraksha Sanhita" introduces coercive measures for summons, warrants, and audio-video recorded searches in "Sections 94, 96, and 105." Meanwhile, the "Bharatiya Sakshya Adhiniyam" offers rules for admissibility and integrity of electronic records in "Sections 61 to 63," with guidelines on secure records and signatures in "Sections 85 and 86." Moving forward requires careful adjustments at each point in this system so that the concepts of necessity, proportionality, and purpose limitation are apparent in records, not just in arguments. This means setting clearer boundaries for "certain legitimate uses," stricter warrant standards for device searches, an independent and skilled Board, better consistency with the Information Technology Act regarding identity offenses, and a research program that monitors decisions and outcomes rather than relying on impressions.

9.1 Calibrating Legitimate Uses

Section 7 of the DPDP Act, 2023, categorizes non-consent grounds as “certain legitimate uses.” This list includes voluntary provision for a specific purpose, compliance with the law, State functions related to sovereignty and security, benefits delivery, employment situations, and other defined cases. You should push for clearer wording in the rules and for stronger documentation requirements in guidance. This way, each use will have a clear aim, a narrow data scope, and measurable safeguards. The structure of the statute allows for this without rewriting the Act. The Central Government can create rules that require purpose statements to specify the legal basis, the minimal data fields, retention periods, and review checkpoints. Fiduciaries can be required to keep internal assessments that explain why consent would be impractical or misleading and how risks are reduced in practice. The Board can then handle disputes by examining those assessments, notice texts, and deletion proofs instead of depending on vague assurances. This approach respects the Act’s design while matching it with the necessity and least restrictive means standard that came from the constitutional changes in 2017. It also gets ready for predictable audits in both public and private processing that rely on records, not just words.

9.2 Surveillance and Device Seizure Standards

Digital era investigations need clarity that matches their intrusiveness. “BNSS Section 94” covers summons to produce documents or other items. “BNSS Section 96” outlines search warrants, and “BNSS Section 105” requires recording search and seizure using audio, video, or electronic means. You should push for warrant templates that clearly state the purpose, detail

the types of devices or accounts involved, describe the categories of data sought, and outline steps for minimizing data collection, such as on-device screening or targeted extraction. Execution protocols should document hash values, time stamps, and limits on scope. Audio and video capture should link to an evidence package that the “Bharatiya Sakshya Adhiniyam” can receive under “Sections 61 to 63” along with the Schedule certificate. When privileged or third-party data is likely, neutral filtering or staged review orders can be included in the warrant. These details do not slow down investigations. They help reduce over-collection, lower chain of custody disputes, and ground the necessity in the warrant's text and the record of its execution. Courts and the Board can then consider DPDP rights and BNSS powers together. They can ask whether narrower steps were possible, whether the description of sought data was specific, and whether deletion or sealing took place after the search's goal was met.

9.3 Board Independence and Capacity

The "Data Protection Board of India" under "Section 18 of the DPDP Act, 2023" connects rights on paper with meaningful remedies. You should support measures that secure appointments, tenure, and funding. This will ensure decision-making remains independent and separate from daily executive preferences. Transparent procedures are as important as formal independence. Publish templates for complaints, breach notices, and voluntary commitments. Regularly provide reasons for classifying breaches and establish penalty ranges based on severity, duration, and resolution. Create an internal technical team that can examine logs, interpret DPIAs, and evaluate claims of anonymization or de-identification. Encourage digital proceedings, but keep the option for oral hearings in complex cases. When the Board establishes consistent standards for "certain legitimate uses," consent withdrawals, and the timing and content of breaches, fiduciaries will adjust their programs accordingly. Over time, a series of decisions will create a reliable guide for proportionality in data processing, similar to how the "Bharatiya Sakshya Adhiniyam" provided a dependable guide for electronic proof.

9.4 Harmonization with Sectoral Laws

Privacy practices can struggle if DPDP duties move away from sector-based controls. The easiest improvements come from aligning fraud prevention with user safety. Identity theft and impersonation are already addressed in “Section 66C of the Information Technology Act,

2000" and "Section 66D of the Information Technology Act, 2000." Processing signals for fraud detection or platform integrity often falls under "Section 7" as non-consent use related to legal compliance or user protection. You should make this connection clearer through joint advisories that describe the legal basis, the minimum signal set, retention periods, and methods for sharing with law enforcement that comply with "BNSS Section 94" or a warrant under "BNSS Section 96." The "Bharatiya Nyaya Sanhita" defines privacy-protective offenses, such as revealing a victim's identity or sharing images without consent. Platforms can align their takedown and reporting processes with both DPDP and BNS by grounding processing in "Sections 5 to 7" and keeping "BSA" compliant evidence packets under "Sections 61 to 63." This strategy prevents overlap and under-enforcement, improves user outcomes, and clarifies things for auditors who need to assess purpose, scope, and safeguards.[22]

9.5 Litigation and Research Agenda

A credible research agenda should track how doctrine meets operations. Start with a database of Board orders under "Section 18." Code these for issues like consent withdrawal, reliance on "Section 7," breach timing and content, and penalty calibration. Link those outcomes to design choices in notices, dashboards, and DPIAs. This lets you connect posture and results. At the same time, monitor High Court decisions reviewing "BNSS" device seizures for the sufficiency of details, adherence to "Section 105" audio video recording, and respect for minimization. Include "BSA Sections 61 to 63" by logging how often courts reject electronic evidence due to certificate defects and what fixes they accept. Over time, this dataset will show whether DPDP rules and guidance achieve proportionality in practice or if certain legitimate uses need clearer boundaries. The Supreme Court's review of rules could then rely on actual patterns instead of assumptions. This would help link constitutional privacy with a processing framework that demonstrates its restraint in records, not just in words. This is how you make the transition from principle to practice credible across platforms, agencies, and courts.

10. SUGGESTIONS

Building on the analysis of From Puttaswamy to DPDP 2023: Continuity and Contradictions in India's Privacy Jurisprudence, the following measures can improve implementation and

[22] Information Technology Act, 2000, available at: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited on September 25, 2025).

resolve tensions.

• Tighten Section 7 "legitimate uses" through rules requiring purpose statements, minimal data fields, and retention horizons. This ensures that non-consent processing remains aligned with proportionality.

• Develop model warrant templates under BNSS Sections 94 and 96 that specify device categories, data scope, and minimization steps. Courts and investigators can then apply proportionality visibly in execution.

• Establish appointment and tenure safeguards for the Data Protection Board under Section 18. A transparent process will reinforce independence and build public trust. • Require Significant Data Fiduciaries under Section 10 to publish anonymized DPIA summaries. Public visibility of risk assessments will improve accountability without disclosing sensitive details.

• Issue joint advisories mapping DPDP Section 7 with IT Act Sections 66C and 66D for fraud detection. This harmonization avoids duplication and clarifies lawful bases for processing.

• Mandate standardized consent withdrawal interfaces under Section 6 with parity in ease to granting consent. Regulators can test compliance through periodic audits of consent flows.

• Expand AV-recording standards in BNSS Section 105 to require cryptographic sealing of search videos. This preserves evidentiary integrity while bolstering privacy safeguards.

• Align children's data protections under Section 9 with platform-level obligations to deploy age-appropriate design codes. This reduces risks from profiling and targeted advertising.

• Require DPDP-compliant breach notices to include log extracts and remedial timelines. Linking breaches to evidentiary-ready artefacts supports both accountability and courtroom reliability.

• Create a research repository of Board orders, High Court rulings, and BSA evidence

exclusions. Such empirical mapping will reveal whether proportionality is functioning in daily practice.

CONCLUSION

The journey from K.S. Puttaswamy v. Union of India (2017) to the Digital Personal Data Protection Act, 2023 shows how India has moved from viewing privacy as a basic right to establishing a clear set of rules for managing data in daily life. Puttaswamy focused on dignity, autonomy, and proportionality as key constitutional principles. The DPDP Act turns these principles into practical measures. It outlines specific roles in Section 2, details rights in Sections 11 to 13, and sets up enforceable duties, which carry penalties through the Data Protection Board of India. The legal framework BNSS on summons and search, BSA on evidence acceptance, and BNS on digital crimes—ensures privacy is not only about individual rights. It also serves as a practical limit on both the State and private entities. Together, these tools create a governance model where proportionality and necessity must be evident in consent processes, warrants, and certificates, rather than just debated in court.Yet, the transition also shows contradictions. The Act balances independence with administrative ease by expanding "certain legitimate uses" under Section 7 and allowing broad exemptions for State functions. This could weaken the proportionality test that Puttaswamy required. The independence of the Data Protection Board, the clarity of warrant standards under BNSS, and the precision of evidentiary rules under BSA will determine if constitutional privacy principles are upheld in practice or undermined by legal shortcuts. Ultimately, the framework's strength relies on how well regulators, fiduciaries, and courts handle consent, accountability, and evidence to ensure that rights remain meaningful, not just symbolic.