DIGITAL PRIVACY, DATA PROTECTION, AND THE FUTURE OF INDIAN DEMOCRACY: A CRITICAL POLICY ANALYSIS OF THE DPDP ACT 2023 AND DPDP RULES 2025

(CASE REPORT BY DEVANSHI MEHTA)

ABSTRACT

This report examines India's new Digital Personal Data Protection (DPDP) Act 2023 and accompanying DPDP Rules 2025 through legal-doctrinal, comparative, and analytical lenses. We analyse the Act's provisions (consent, data-principal rights, fiduciary duties, exemptions, localisation), identify critical gaps (consent asymmetries, broad state powers, digital divide, enforcement weaknesses), and assess democratic risks (surveillance, chilling of dissent, transparency deficits). Historical context (from global privacy norms to the Puttaswamy judgment and Aadhaar cases) frames the discussion. Comparative analysis considers GDPR (EU), CCPA (California), and data governance in Germany, France, and South Korea. We propose innovations and best practices (data audits, public literacy drives, data trusts, and transparency tools) and outline a policy roadmap to strengthen India's digital safeguards while preserving democratic values. Key findings include that while the DPDP Act formally recognizes data rights, sweeping exemptions for the state, weak enforcement architecture, and persistent inequalities risk undermining privacy protections. The report concludes with recommendations to reconcile India's welfare-democratic identity with robust digital rights and outlines likely developments over the next five years.

Keywords: DPDP Act 2023, Consent, Surveillance, State exemptions, Data fiduciary, Digital divide.

INTRODUCTION

The **digital transformation of governance** and society in India has accelerated dramatically. By early 2025, India's 1.46 billion people accounted for roughly 806 million internet users (55.3% of the population) and 491 million social media accounts. Mobile phones are ubiquitous – 1.12 billion cellular connections (76.6% penetration) and 96% of internet access via mobiles

(6h49m of daily online time) highlight a predominantly mobile-first nation. Yet this **expansion is uneven**: only about 44.7% of Indians remained offline in 2025, disproportionately in rural and marginalized communities (e.g. only ~16% of rural vs ~48% of urban households had internet by 2016). *Figure 1* (below) highlights the overall adoption and use of connected devices and services. We also observe state-level internet penetration: Kerala, Goa, and Maharashtra lead (~70%), while Bihar, Uttar Pradesh, and Jharkhand lag below 50%. This **digital divide – by geography, gender** (rural women ~22.9% computer-literate vs 32.3% men), and **socio-economic status – constrains equal participation in digital democracy.** Compounding this, a 2025 survey found 86.3% of households have internet and ~96% of 15–29-year-olds own smartphones, yet significant urban–rural and gender gaps persist (rural female smartphone ownership ~75.6% vs urban female ~86.2%). Thus, **digital inequality** remains a pressing structural challenge.

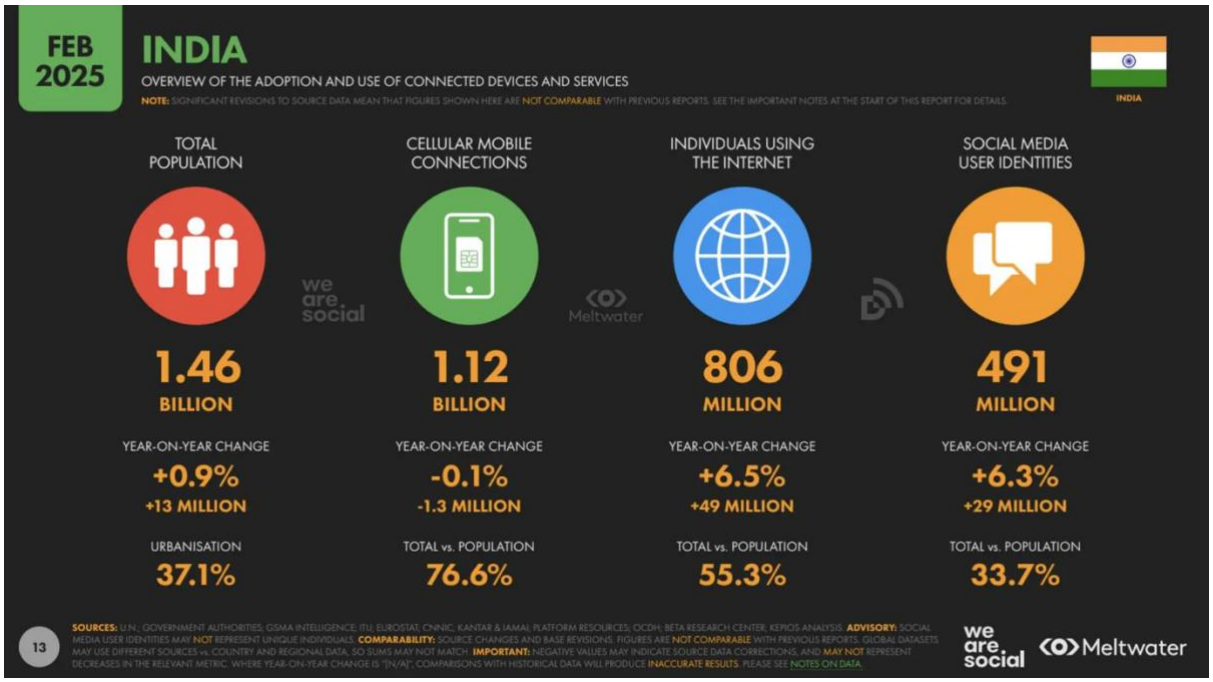

Figure 1: India (2025) – population 1.46B; 806M internet users; 491M social accounts (55% and 33.7% of population respectively).

India's democracy – the world's largest – has seen major upheavals (religious and caste-based politics, agrarian distress, urban protests) even as the state deploys digital tools (Aadhaar biometric IDs, e-governance portals, surveillance, counter-terrorism databases). The **Supreme Court's landmark Puttaswamy decision (2017) enshrined privacy as a fundamental right under Article 21**, reflecting that citizens' informational autonomy is central to life and liberty. Yet practical privacy safeguards have struggled: Aadhaar's Supreme Court approval (2018) was limited to welfare schemes and required stringent proportionality tests. In politics, **emerging use of personal data is reshaping electoral practices**: for example, parties have harvested government welfare and Aadhaar-linked databases to micro-target voters, resulting in a **2019 scandal where an app called Sevamitra illegally accessed 7.8 crore voters' Aadhaar-linked data for campaigning.** More recently, young voters in Bengaluru reported unsolicited calls from parties across India, and a major party inadvertently posted a screenshot

of its access to beneficiaries' personal data. These episodes illustrate how digital data can entrench identity politics and undermine free and fair elections.

Datafication also intersects with India's constitutionally contentious issues: caste data and political representation. In mid-2024 the Union Cabinet cleared the first nationwide caste census (NDRC) in 70 years, slated for the 2027 Census. This has reignited debates on constituency delimitation and reservation quotas. Bihar's 2022 caste survey (unofficially tallied) was quickly followed by a political promise to expand OBC quotas, suggesting that granular caste data can be used to rapidly reshape welfare policy and representation. Experts caution that **caste information is sensitive personal data – prone to leaks and misuse against marginalized groups – yet lacks strong privacy safeguards.** Thus, how India's emerging data regime treats caste, religion, and ethnicity will have major democratic implications.

At the same time, civic dissent, and digital speech face growing constraints. **Independent organizations warn of an "appalling lack of transparency" in how the government blocks online content.** For example, over the last decade hundreds of news sites (especially in Kashmir and protest movements) have been arbitrarily banned under cybersecurity rules. Reporters without Borders notes that amendments to India's IT rules (2021) enable "the tightest possible control of the Internet and social media". Mandatory data localization and encryption regulations, combined with the looming threat of a surveillance state, risk chilling free expression. In late 2025, India briefly attempted to mandate a government **"Sanchar Saathi"** telecom data app on all smartphones, prompting alarm from former Supreme Court justices that such forced tracking "fails the Puttaswamy test" and is akin to placing a CCTV in every room. These conflicts – between the state's development and security agenda vs individuals' privacy, between welfare policies vs caste/identity entitlements, and between information control vs free mobilization – frame our inquiry.

HISTORICAL AND LEGAL FOUNDATIONS

India's journey toward modern data protection has unfolded over decades, paralleling global trends. Internationally, the notion of privacy gained legal traction in the 20th century (e.g. 1890 Harvard Law Review "right to be let alone" concept), but only in the 2010s did comprehensive frameworks like the EU's GDPR (2018) emerge. In India, statutory provisions have been piecemeal. **The Information Technology Act, 2000** (amended 2008) introduced Section 43A requiring sensitive data security practices by corporations. Still, there was no enforceable personal data law until the late 2010s.

A crucial turning point was the 2017 Supreme Court decision in **Justice K.S. Puttaswamy v. Union of India**. A nine-judge bench unanimously held that the **right to privacy is a fundamental right under Articles 14, 19, and 21 of the Constitution.** This sweeping judgment recognized informational privacy (including personal data) as intrinsic to dignity and

liberty. It set out a three-part test for surveillance and data collection: **legality** (a law must authorize the intrusion), **necessity** (a legitimate state purpose, like crime prevention or welfare), and **proportionality** (least intrusive means). The Court explicitly warned against unchecked state data collection, emphasizing the need for robust legal safeguards.

Simultaneously, the Aadhaar biometric ID program led to landmark cases. In **Puttaswamy-II (2018)**, the Court upheld Aadhaar's use for welfare subsidies but struck down its mandatory linkage for telecom or private services. It upheld privacy constraints: minimal data usage and consent for enrolment. The Court's proportionality test applied: Aadhaar's benefits were outweighed by risks if misused outside its narrow welfare mandate. These rulings spurred demands for a comprehensive data law.

Responding to the judicial mandate, the government formed the **Srikrishna Committee (2017–2018)** chaired by Justice B.N. Srikrishna. Its July 2018 report proposed India's first draft data protection legislation. Drawing on international models, it recommended a **"data fiduciary" framework**, mirroring GDPR's data controllers but defined under Indian law. Key principles included consent for all personal data and explicit consent for **"sensitive personal data,"** the latter including caste, religion, sexual orientation, health, biometrics, etc. . . . For instance, caste and religion were designated sensitive, requiring special consent. The Committee also endorsed individual rights (notice, access, correction, erasure, data portability). Its blueprint mandated purpose limitation and security safeguards, with an **independent Data Protection Authority (DPA)** to supervise compliance. Notably, it drew on fiduciary duty concepts: data-handlers must "deal fairly" and process data only for authorized purposes.

Based on these recommendations, the first **Personal Data Protection Bill (2019)** was tabled in Parliament. It largely followed the Srikrishna model, including **GDPR-style features** like DPIAs for high-risk processing, localization, and severe penalties. However, it was never enacted. A Joint Parliamentary Committee reviewed it, and a 2022 version was proposed, but intense debates (over state data use, non-personal data, inter-state data flows) stymied progress.

Meanwhile, global practice continued evolving. The EU implemented GDPR in 2018, setting standards like data protection by design, breach notification, and hefty fines (up to 4% of global revenue). The U.S. saw a patchwork approach with California's CCPA/CPRA granting opt-out of sale and private enforcement (though India's DPDP Act lacks any private right of action for citizens). Countries like Germany and France, under GDPR, emphasize independent regulators (e.g. CNIL in France), mandatory Data Protection Impact Assessments, and strong transparency requirements (e.g. DPIAs, data breach notifications). South Korea's Personal Information Protection Act (2011, strengthened 2020) is often cited as one of the world's strictest: it defines "sensitive information" expansively (including thoughts and beliefs) and allows the independent PIPC to levy heavy fines (Meta was fined $15.6M for unauthorized sharing).

Back in India, the stalemate ended in August 2023 when Parliament passed the **Digital Personal Data Protection Act, 2023**. Coming six years after Puttaswamy, the law aimed to

operationalize privacy rights in a way consistent with the Constitution. Alongside, the government framed draft rules, which were notified in final form (**DPDP Rules, 2025**). This new regime represents India's first statutory data protection framework.

Key legal foundations include: Consent as the default rule (every processing requires free, informed consent, withdrawable at any time); Data Principal rights (to information, correction, portability, erasure, grievance redressal, and nomination) for living and deceased individuals; Data Fiduciary obligations (security safeguards, minimal data collection, breach reporting); and Broad exceptions for state functions, research, and emergencies. Importantly, unlike earlier drafts, the DPDP Act notably softens data localization: it does not mandate data be stored only in India. Instead, cross-border transfers are allowed unless specifically restricted by government notification.

In sum, India's privacy framework evolved from Puttaswamy's constitutional recognition to a formal law in 2023. The DPDP Act diverges from its predecessors by accommodating India's digital economy and asserting certain state prerogatives. The following sections scrutinize these provisions in detail.

DPDP - KEY PROVISIONS

The DPDP Act 2023 and its 2025 Rules establish a consent-based data regime with several new terms and obligations. We outline its core features:

- **Scope and Definitions**: The law regulates **"digital personal data"** – data about an identifiable individual (data principal) that is collected in electronic form. It does not cover offline data or non-personal data (though anonymized statistics are exempt). It **excludes "publicly available personal data"** (anything the individual themselves has made public). Entities determining the purpose/means of processing are "Data Fiduciaries;" significant players (like major social media, search, and e-commerce platforms) are classified as **Significant Data Fiduciaries (SDFs)** and subject to extra duties. The Act applies to any data fiduciary collecting data in India or outside India for offering goods/services within India, thus having extraterritorial reach like GDPR.
- **Consent Architecture**: Processing is lawful only with the data principal's consent, which must be free, specific, informed, and unambiguous. **Consent** must be obtained before or at the time of data collection. Principals have the right to withdraw consent at any time in a similar free and simple manner. Importantly, **no alternative legal bases** (like contractual necessity or legitimate interests) are provided – all processing is consent-bound. The Act requires **clear privacy notices in plain language (Rules 3–4)** explaining what data is collected and why. As in GDPR, implied or bundled consent (e.g. "accept all cookies" without choice) would not qualify as valid. Unlike some earlier drafts, **the Act does not have a specific "child data" consent mechanism under central rules**, though the Rules do require parental permission for below-18.

- **Data Principal Rights**: The Act codifies several rights for individuals: **the right to notice** (information about processing); **access** (obtain details of data held); **correction** (amend inaccurate data); **erasure** (withdraw consent and delete data, akin to 'right to be forgotten'); **data portability** (receive a copy of data in machine-readable form); **grievance redressal** (complaints to fiduciaries and to the Board); and **nomination** (designating someone to handle their data after death). These empower citizens to control their data. Fiduciaries must provide simple mechanisms (portal, email etc.) to exercise these rights **(Rule 14)**. There are defined timelines: fiduciaries must respond to rights requests within 30 days. However, the law conspicuously does not provide for a private lawsuit by individuals for breaches or non-compliance – enforcement lies exclusively with the state-appointed Data Protection Board.
- **Fiduciary Obligations**: Every data fiduciary must implement **"reasonable security safeguards"** to protect data. **Breach reporting is required**: fiduciaries must notify the Board of any data breach within 72 hours, and all affected principals within a reasonable time. They must not process data beyond the stated purpose, must delete data when no longer needed for lawful purposes (storage limitation), and must maintain records. **Significant Data Fiduciaries have additional duties (Rule 13)**: they must conduct annual Data Protection Impact Assessments and audits, and ensure their algorithms and technical processes do not harm user rights. They must store certain critical data for at least three years as per rules (e.g. telemarketers must keep call logs). All fiduciaries must establish a **grievance redressal officer** (who must reply within 90 days) and clearly publish how users can exercise rights (identifiers needed, methods, timelines).
- **Exemptions and State Powers**: The Act contains extensive exemptions that carve out state interests. Processing done "in the interests of the sovereignty or integrity of India, security of the State, friendly relations with foreign states, public order, or preventing incitement" is entirely exempt. In practice, this means intelligence agencies, police and other security bodies are largely outside the law's ambit. Additionally, data processing for "archival, statistical or research purposes" is exempt if no individual-specific decisions are made. The **government may also exempt classes of fiduciaries** (e.g. small startups) from certain provisions (notice, accuracy, etc.).

  A particularly controversial clause allows the Union Government, by notification, to exempt any data fiduciary or class from any provision of the law for up to five years. This grants a broad discretionary power with no stated limits, effectively allowing the executive to suspend obligations at will. Moreover, **central officials can compel fiduciaries to provide personal data on vague grounds: Section 36 of the Act (reflected in Rule 23) lets the government demand data from fiduciaries if it deems it necessary** for the above **state interests.** The fiduciary must comply within a fixed (often short) timeframe, and even bar itself from informing the principal. Critics argue these exemptions are too sweeping and could swallow the rule of law.

- **Data Localization**: Unlike the draft 2019 bill, the final **DPDP Act does not mandate all personal data be stored in India**. It simply empowers the government "to restrict" cross-border data transfers by notification. Thus **foreign-to-India companies may**

currently transfer data overseas unless the government explicitly bans certain destinations. Sectoral rules (for example, RBI norms on payment data) remain unaffected. For most private businesses, transfers are allowed once the Rules come into effect, though fiduciaries must register (within two years) with the Board. This liberal approach **facilitates global trade** but also **raises concerns** about **sufficient oversight of international data flows**.

- **Regulatory Authority**: The Act establishes the **Data Protection Board of India (DPB)** as the enforcement body. The DPB has a Chairperson and Members appointed by the government. However, its powers are limited. The Board can inquire into complaints, order fiduciaries to remediate breaches, and impose penalties (up to ₹250 crore). Notably, the **Board cannot issue binding regulations** or guidance to firms, a sharp break from GDPR-style Data Protection Authorities. It also **cannot supervise all data processing** – it acts reactively. In this way, the DPB is more akin to a compliance tribunal than a proactive regulator. Appeals from DPB orders lie with the existing **Telecom Disputes Settlement and Appellate Tribunal (TDSAT)**.

In summary, the DPDP Act builds a framework of consent and rights, drawing on global models. Yet its true impact depends on the many gaps and implementation details: wide exemptions for the state, limited regulator powers, and staggered rule-making (many obligations begin years later). The following section explores how these features create risks to democracy and rights.

CRITICAL GAPS AND DEMOCRATIC RISKS

While the DPDP Act marks progress, several gaps and risks raise alarms for democracy and civil liberties:

- **Consent Asymmetry and Consent Fatigue**: Although consent is central, real-world **consent may be illusory**. Critics note that most online services will still rely on **"take-it-or-leave-it" terms**, with few viable alternatives for citizens. Many **young users simply "accept" privacy policies without understanding them**: a **survey** of Indian teenagers found ~80% had little grasp of what a data breach meant, and ~90% never read privacy policies. In practice, consent often means a bureaucratic tick-box, reinforcing an asymmetry where data fiduciaries hold all the information. This imbalance worsens when rules **allow default sharing**. For instance, the DPDP Rules permit fiduciaries to require SIM verification for users and to track data without notifying individuals in certain cases. This consent fatigue **erodes genuine privacy control**.
- **Sweeping Surveillance and Security Powers**: The **Act's state-centric exemptions effectively place the government above the law.** Under **Section 36 and Rule 23**, officials can demand any citizen's personal data on grounds like "national security" or "public order," **without judicial oversight**. There are **no clear standards or appeal**

rights – only an obligation on fiduciaries to comply (or face penalties). This asymmetry means ordinary people are shielded by consent, but the state is not. Observers warn that such provisions create a **"surveillance blowback"**: even legally rationalized surveillance can chill dissent and privacy (the **"panopticon" effect**). Notably, multiple justices of the Supreme Court urged caution in the **Sanchar Saathi case**: Justice A.K. Sikri observed that mandatory data collection "fails the proportionality test" of Puttaswamy. Experts fear that **new digital ID initiatives** (e.g. health data IDs, RBI digital rupee identifiers) combined with DPDP exemptions could lead to **quasi-compulsory data harvesting without recourse**.

- **Digital Divide and Algorithmic Bias**: The law is technology-neutral on paper, but **in practice only the digitally connected can exercise rights**. Rural and low-income citizens, many of whom may not fully grasp privacy concepts, might inadvertently lose out. For example, some UID-linked welfare schemes require Aadhaar authentication. If citizens lack awareness of rights, they have limited capacity to contest misuse. Meanwhile, **algorithmic governance** (credit scoring, social service eligibility, law enforcement profiling) can **perpetuate bias**. The **DPDP Act does not impose independent algorithmic audits or fairness obligations beyond internal fiduciary assessments**. Thus, opaque profiling by private platforms or government 'AI tools' remains unchecked. In effect, the **Act preserves the status quo**: entrenched **digital inequalities** will likely persist unless supplemented by affirmative measures (e.g. targeted literacy or public interest data sharing).
- **Enforcement Weakness and Conflict of Interest**: The Act's reliance on a **government-appointed Board** is problematic. Unlike GDPR DPAs or South Korea's PIPC, India's DPB lacks rulemaking power and complete independence. Its **chair and members are chosen by the executive (via MeitY)**, raising questions of impartiality. Budget, staffing, and process details are in rulebooks, not statute, leaving ample room for delay. The Board only enforces after complaints or breaches – there is **no proactive auditing**. This could lead to a **weak enforcement culture**, especially since **large government-linked companies** (which theoretically should comply) **are not clearly disciplined** by the Board. The fact that fiduciaries themselves (e.g. telecom operators) were pressed to provide data for Sanchar Saathi without court orders indicates how easily the boundaries of enforcement can be overrun by politics. Observers note a **"transparency imbalance"**: citizens have rights in name, but no meaningful oversight exists for how the state or big tech exercise data powers.
- **Threats to Dissent and Press Freedom**: The interplay of DPDP exemptions and other laws creates chilling effects. Under the Rules, **news media personnel** fall under the broad definition of **"data fiduciaries,"** meaning journalists' notes and recordings could **in theory be regulated**. Moreover, the Act's bar on publicly available personal data (exemption to privacy) has drawn fire: the 2025 Rules expand **"public interest"** exceptions in ways that critics fear will gag investigative reporting. For example, publishing leaked data about politicians could be stifled under **ambiguous "sovereignty" grounds**. As the Editors Guild warned, compulsory registration of data collectors (like news sites) and the threat of ₹500 crore fines for breaches could "**impede routine reportage and chill accountability journalism**". In practice, any

protest organizer or opposition figure leaving a digital trail might risk state scrutiny without remedy. The **digital dissemination of dissent** (social media posts, encrypted chats) faces potential oversight without meaningful checks. Combined with stringent "fake news" rules, these DPDP **loopholes** pose a **danger to free expression** in a vibrant democracy.

- **Transparency and Archival Memory**: A robust democracy relies on public information. Yet ironically, the Act's scope and exclusions may **hamper transparency**. Since **"publicly available" personal data is exempt**, it seems that even if a legislator's contact info is published in official documents, the Act might not protect how that data is processed (a **privacy blind spot**). Even more troubling, the proposed **Section 37** in the Act, allows the government to block public access to any service from a fiduciary that the Board penalizes twice. In effect, a company could be cut off from providing any online goods or services if it falls afoul of one of the loosely defined rules twice. This unknown **"internet kill switch"** (like France's DSA "digital blackmail" proposals) risks de-archiving and censoring without judicial review. While ostensibly aimed at repeat offenders, critics have noted that the criteria ("**any two penalties**") are not narrowly tailored. Such an authority undermines transparency for citizens who rely on digital platforms for information and commerce.
- **Algorithmic Opacity**: The **law touches little on AI and algorithms**. Fiduciaries must ensure their **algorithms "do not harm user rights," but no clear standard or audit is prescribed**. There is no requirement for explainability or public scrutiny of automated decisions. This gap is acute as India launches **AI-driven services** (AI-based KYC, credit scoring, and city surveillance analytics). **Without enforceable guidelines or external audits, algorithms remain black boxes**. This not only **risks privacy** (profiling at scale) but also **accountability**: a wrong automated decision (e.g. false match in face recognition) can have no remedy under the DPDP Act.

In sum, the **democratic risks** are significant. The DPDP framework, while formally modern, contains deep flaws. The consent-centric approach risks being cosmetic in practice. State exemptions effectively create a dual system – one for citizens, one for the state – that many legal scholars warn violates the spirit of Puttaswamy. The burdens on the press and civil society suggest a tilt toward surveillance and control, justified by vague national interest. Without strong democratic safeguards, citizens may find that their new privacy rights exist more on paper than.

JUDICIAL AND POLICY VIGNETTES

Historic court decisions have shaped India's data landscape through the following cases -

- **Puttaswamy v. Union of India (2017)**: As noted, this **nine-judge judgment** was a watershed, affirming privacy as a pillar of **liberty**. It laid down a test to evaluate any data collection or surveillance law against constitutional norms. Importantly, it

recognized "**informational privacy**" – control over one's personal data – as integral to **dignity**. The decision insisted any deprivation of privacy must serve a legitimate aim (like public health or welfare) and be proportionate. This case provides the reference point for all critiques of the DPDP Act: **if privacy is fundamental, how can laws exempt so much of government activity?** Judges on Puttaswamy's panel later warned, in Sanchar Saathi, that putting spyware on citizens' phones "fails every test" established in the 2017 case.

- **Aadhaar (2018)**: In Justice K.S. Puttaswamy (No. 2), a nine-judge bench upheld the **constitutionality of Aadhaar** for **welfare schemes**, **imposing strict privacy conditions**. The Court held Aadhaar is not mandatory for all services, underlining that state data collection must be limited to stated purposes. The Court also held that **biometric data** is "**sensitive personal data**" deserving heightened protection (anticipating later PDP frameworks). These rulings implicitly informed the DPDP Act's structure (e.g. special mention of biometric and sensitive data, restrictions on linking Aadhaar beyond welfare).
- **Sanchar Saathi Case (2023–2025)**: This recent episode vividly illustrates the clash of digital policy and privacy law. In late 2023, India's **Department of Telecommunications** issued a directive that all telecom operators integrate a new "**Sanchar Saathi**" app and compel users to install it. The app would allow subscribers to see details of calls and SMS routed via their number. Ostensibly for "**cybersecurity**," this effectively meant every phone had to have state-monitored connectivity records. After a massive **public outcry** and **legal pushback** (including letters from several former Chief Justices), the government reversed course in December 2025, declaring installation voluntary. During this incident, **former Supreme Court justices** were vocal: Justice B.N. Srikrishna likened forced installation to "putting a CCTV in every room." Justice A.K. Sikri stressed the measure was not the least restrictive means and violated the Puttaswamy proportionality test. These judicial critiques underscore that even rules outside DPDP (under telecom laws) raise **Article 21** issues. Ironically, the DPDP Act was also invoked: rule-makers claimed Sanchar Saathi aligned with the Act's framework, but critics noted it directly conflicted with the Act's **consent requirement**. The episode demonstrated the limits of DPDP's influence: it did not prevent the attempt, but public and judicial pressure forced policy change. It also served as a cautionary tale: technology-enabled surveillance will be challenged on privacy grounds.
- **Other Judicial Discussions**: Though Sanchar Saathi has not yet resulted in a final judgment, it generated policy pronouncements by courts about digital rights. Separately, in **2023 a Punjab & Haryana High Court held that URL tracking by the government (for content moderation) must meet Puttaswamy's tests**. Similarly, **disputes over government health apps (CoWIN for vaccines) in 2021 prompted courts to emphasize data minimization and user consent**. These vignettes collectively signal that India's judiciary remains vigilant: any perceived drift by the executive into mass data collection is likely to trigger Puttaswamy-style scrutiny.

In policymaking, too, signals have been mixed. Justice Srikrishna (former Committee chair) publicly warned that the DPDP Act's broad exemptions risk turning it into a "split-level bridge," protecting private data but not state data, which he argued was unconstitutional. Civil society organizations (Internet Freedom Foundation, Editors Guild) have mounted legal challenges against the DPDP Rules, contending they overstep legislative intent and endanger press freedom. On the legislative front, some amendments (e.g. requiring social media firms to hand over user data to government on request) suggest an uneasy compromise between digital rights and perceived national interest. In all, **judicial and policy debates highlight tension**: India has recognized privacy but struggles to embed it across all domains of governance.

COMPARATIVE DEMOCRATIC PRACTICES

To gauge India's DPDP regime, it helps to compare with **other democracies' data laws and governance models**. Key contrasts include:

- **EU / GDPR**: The **EU's General Data Protection Regulation (2016/18) is often the** gold **standard**. It grants fundamental rights to data access, erasure, portability, and explicit consent for any processing. It introduces principles like privacy by design, data minimization, and data protection impact assessments (DPIAs) for high-risk activities (none of which are explicit in DPDP aside from SDF audits). Enforcement in the EU is through **independent Data Protection Authorities** (DPAs, e.g. France's CNIL, Germany's BfDI) with broad investigative powers (audit companies, issue binding orders). The **GDPR has already generated tens of billions of euros in fines** (e.g. Meta and Google repeatedly penalized for violations). For example, in September 2025 France's CNIL imposed a €325 million fine on Google for processing Gmail data and cookies without consent – a high-profile case of strict enforcement. India's DPDP law, by contrast, empowers the state rather than an independent regulator to police compliance, and caps penalties at ₹250 crore. While the Act uses a consent-based approach akin to GDPR, it does not allow other lawful bases (like contractual necessity or legitimate interests), making it uniquely consent-heavy. Notably, GDPR requires prompt breach notification to both authorities and affected users; the DPDP Act requires reporting to the Board but not necessarily to individuals. Finally, GDPR includes a private right of action and litigation option (including class actions) for data subjects, which DPDP lacks entirely.
- **United States / CCPA**: The **U.S. has no single federal privacy law (as of 2025), but California's CCPA/CPRA extends strong rights to residents**: right to know and delete personal data, opt-out of data "sales," and protection against discrimination for exercising rights. Enforcement is by the **state AG and allows citizen lawsuits for certain breaches**. DPDP's rights (access, portability, deletion) are similar in spirit, but it has no consumer lawsuit mechanism – only the state-board enforcement. Also, India's Act does not define "sale" of data (irrelevant, since most data flows through consent managers), so there is no direct opt-out of data commercialization. In practice, a

Californian can sue a company for misuse; an Indian data principal can only complain to the DPB.

- **Germany & France**: As EU members, these countries follow GDPR but add national nuances. **Germany's Federal Data Protection Act (BDSG) and France's 1978 Data Protection Act** impose additional safeguards. Both nations protect privacy as a constitutional value and ensure very strong sectoral regulations (like health, employment). For example, a European concept is "**informationelle Selbstbestimmung**" (informational self-determination) in Germany – close to Puttaswamy's notion. In practice, **Germany's multiple Länder DPAs and France's CNIL** actively audit government projects, require algorithmic transparency, and mandate human oversight on AI in sensitive sectors. An illustrative difference: in Europe, any project using personal data for profiling often triggers a mandatory DPIA and supervisory authority approval – a safeguard India's law lacks.
- **South Korea (PIPA)**: **Korea's Personal Information Protection Act (PIPA)** is widely regarded as one of the strongest. It requires explicit consent for any processing of personal data and strict conditions for sensitive information. The law explicitly covers non-human data subjects and has criminal penalties. Its regulator, the **Personal Information Protection Commission (PIPC)**, is independent and has **imposed multi-million-dollar fines**. For instance, in **2024 PIPC fined Meta ~$15.6M** for sharing user data without consent. Korea also mandates that data breach notification must reach affected individuals promptly, and it even bans any arrangement with foreign companies to circumvent consent. By comparison, India's law gives broad leeway to state authorities that PIPA would never allow – e.g., PIPA explicitly prohibits collecting ethnic background or belief data without permission. In sum, Korea shows that a **dynamic**, **independent enforcement** culture can exist even outside the EU.

In short, **India's DPDP Act is modest by these standards**. It grants similar foundational rights as GDPR/CPRA, but lacks their robust enforcement, independent oversight, and flexibility (no legitimate-interest processing, no private action). On the positive side, it aligns India with global norms (consent, data portability, fiduciary duties) in ways earlier Indian proposals did not fully. However, the **DPDP's power imbalance** (state above the law, weak regulator, and consent as sole basis) departs from these comparative models of privacy as an individual right protected against all actors, including the state.

INNOVATIONS AND BEST PRACTICES

To **strengthen Indian data governance**, we highlight promising tools and practices:

- **Transparency and User Empowerment**: Online platforms and data fiduciaries should implement **clear privacy dashboards** showing data usage. For example, EU initiatives require companies to provide privacy notices at point-of-use. India could mandate or encourage **"one-stop" privacy portals** where users can see all consents given and

easily revoke them. Similarly, whistleblower or inspector-general roles (as in some GDPR frameworks) could audit public agencies' data use. India's **proposed Consent Managers** (third-party intermediaries to handle consents) could evolve into open standards that let users transfer consent history between apps.

- **Regular Audits and Certification**: Government and industry should institutionalize **independent audits**. The DPDP Rules already require SDFs to conduct DPIAs and audits annually. These should be **publicized or reported to Parliament**, like how telecom audits are. A **specialized privacy certification for companies** (perhaps run by TRAI or BIS) could incentivize best practices. Think tanks have also suggested creating a **statutory Data Protection Authority separated from the executive** – for converting the DPB into a truly independent regulator with budgetary autonomy.
- **Public Awareness Campaigns**: Given **low digital literacy**, **nationwide privacy education** is crucial. India's **PMGDISHA** program trained 63.9 million rural citizens in basic digital skills by March 2024. These networks (**Common Service Centres**) could incorporate modules on privacy: teaching people how to spot phishing, understand privacy policies, and exercise DPDP rights. Social media (72.3% of Indians are under 35) can be leveraged to spread simple messages (e.g. "Data is power – know your rights under DPDP"). Civil society could celebrate a Data Privacy Day, host hackathons or debates in colleges, and publish findings in regional languages.
- **Safe Data Archiving and Trust Models**: To guard historical memory and sensitive records, India might explore **safe archiving frameworks**. For instance, specialized archives for health, caste, or security data can operate under strict governance (with oversight boards, like how NIH trusts health research data). The concept of data trusts – legally binding entities that manage personal data on behalf of communities – is being piloted in some countries for health or social research. India could adapt this: for example, a "**Public Health Data Trust**" that anonymizes and vets' datasets on nationwide health, balancing research uses with privacy by design. Similarly, a "**Digital Memory Fund**" might store social media records in encrypted form for historical inquiry (with strong privacy controls). These innovations would require new legal frameworks, but they are worth exploring to ensure public data can serve society without abusing privacy.
- **Regulatory Sandboxes and Collaboration**: India's 2023 Digital Personal Data Protection Rules mention "**sandboxes**" for AI and new tech. The government should indeed promote sandbox environments where startups and civil society co-design privacy-preserving technologies. For example, jointly developing **decentralized identity solutions** (like **blockchain-based IDs**) or **differential-privacy analytics** can reduce reliance on centralized consent models. The private sector can voluntarily adopt "**privacy by design**" (encrypting data at rest, storing minimal PII) and **ethics boards** to review algorithms, following best practices from Europe and Canada.
- **Integrity of Public Data and RTI**: To balance privacy and transparency, India should ensure that the **Right to Information** (RTI) Act operates compatibly with DPDP. Currently, personal data of public officials is exempt from RTI if it invades privacy, but that can be overly broad. **Clear guidelines** can allow release of wrongdoing-related data while protecting family and personal IDs. **Independent commissions** could

oversee de-identified RTI releases. Moreover, as India pushes for open government data, it must anonymize citizen data in published datasets. For example, census or health statistics should aggregate at levels that cannot identify individuals, as is standard in many democracies.

The above are some **concrete ideas**. The guiding principle is privacy-by-architecture: build systems that minimize data collection upfront and distribute control, rather than retrofitting consent forms.

POLICY ROADMAP

Short-term (1–2 years):

1. **Finalize and Clarify Rules**: The government must finalize any remaining rules (for AI, surveillance safeguards, data classification) with maximum transparency. Stakeholder consultations should be meaningful. Key to this is narrowing vague provisions: for example, clearly define "national security" grounds and establish oversight for state access (judicial warrants, legislative oversight) to prevent abuse.
2. **Empower the Data Protection Board**: The DPB's independence should be safeguarded. Appointment rules should ensure a **multi-stakeholder committee** (not just executive picks). The Board should be authorized to issue binding guidance documents and codes of conduct. An **annual DPDP compliance report** to Parliament (like RBI's reports) would bolster accountability.
3. **Build Awareness**: Launch **mass awareness drives** about privacy rights, tied to existing digital literacy missions (PMGDISHA, National Digital Communications Policy). Include DPDP training in school/university curricula, government employee training, and media outreach.
4. **Trial Regulatory Sandboxes**: **Encourage technology sandboxes** in banking (RBI), health (NITI, health ministry), and cybersecurity (MeitY) where privacy-protecting innovations can be tested without full regulatory burden.
5. **Legislative Safeguards**: Consider **Parliamentary review of exemptions**. For example, require any new notification under "sovereignty and integrity" to be laid before both Houses for approval, like emergency law scrutiny. **Increase oversight of Rule 23 orders by an ombudsman or a standing committee.**

Medium-term (3–5 years):

1. **Strengthen Legal Remedies**: Introduce a **private right of action** so that citizens (or class actions) can sue fiduciaries for breaches. This puts pressure on companies to comply. Draw on models like GDPR where individuals can lodge complaints with regulators and have civil remedies.

2. **Harmonize with Other Laws**: **Align DPDP with IT Act amendments** (2021 IT Rules etc.) to avoid contradiction. For instance, **data categories** (children, journalists) should be **consistently defined**. Ensure that any **surveillance laws (like proposed SPY Act or Digital India Act provisions)** explicitly meet Puttaswamy tests, possibly by requiring warrants for data interception.
3. **Achieve International Standards**: Seek adequacy decisions or **bilateral agreements**. Since cross-border data flow is vital, aim to negotiate "**adequacy**" status with the EU or mutual recognition with other democracies based on equivalent protections. This will also enforce DPDP's **credibility**.
4. **Bridge the Divide**: **Invest in rural connectivity** (BharatNet, 5G outreach) and **digital literacy** in tandem with privacy education. Ensure **marginalized groups** (tribal, women, Dalits) have access to **grievance redress channels** (multilingual, low-tech options like toll-free helplines). The goal is **inclusive digital democracy**: rights with reach.
5. **Monitor and Adapt**: The technology landscape evolves (AI, IoT, and genomics). Establish a **high-level committee** (**independent of government**) to review DPDP's adequacy every two years, with **expert inputs**. Adjust the law as needed, e.g. to **cover emerging data forms** (sensor data from IoT, neural data in future).

NEXT 5 YEARS – RISKS AND REFORMS:

If not implemented properly, DPDP risks becoming a bureaucratic checklist. The state might continue parallel data collection under other laws, while citizens remain largely unenforced. We may see a continued patchwork of data protections: e-commerce and finance firms will comply (having international exposures), but many local enterprises and startups will ignore rules until enforcement pressures them. **Judicial challenges** may force incremental curbs on the state's surveillance powers (e.g. courts insisting on warrants for Sanchar Saathi). On the other hand, **strong enforcement abroad** (e.g. fines under GDPR/CCPA) may incentivize Indian multinationals to adopt stricter internal policies globally, indirectly raising domestic standards. The most positive path is if DPDP catalyses a **data protection culture**: mainstream firms adopt "**privacy by default**," citizens become more vigilant (aided by civil society campaigns), and regulators (perhaps a future DPB) take a more active stance.

However, **risks** loom: **geostrategic data localization battles** may re-emerge (e.g. pressures to compel foreign companies to store all Indian data locally). **Crises** (pandemics, security threats) could lead governments to invoke the broad DPDP exemptions and expand data grabs. A failure to narrow these powers could entrench a **surveillance regime under the guise of welfare or integrity**. The **interplay between DPDP and other bills** (like digital competition law, new telecom rules, the proposed IDDPA on digital personal ID) will be **critical** – they could either synergize to create robust privacy architecture or undermine each other.

On balance, the **next five years** will likely see a **mixed evolution**. Key pressure points will be **legal challenges** (courts interpreting DPDP's vague clauses), **civil society activism** (monitoring DPDP implementation), and **international influence** (global tech companies lobbying for harmonized rules). The **recommended reforms** – strengthening independent oversight, expanding rights, and building civic capacity – are urgent to tip the balance toward rights.

CONCLUSION

Reconciling India's **welfare-democratic identity** with a **rights-based digital regime** is the challenge of our time. On one hand, India has shown **global leadership in digital inclusion**: the world's largest biometric ID system (Aadhaar) and massive e-governance platforms have delivered subsidies and services to hundreds of millions. On the other, these same technologies harbour the potential for **intrusive surveillance and data-driven control**. The DPDP Act 2023 and Rules 2025 reflect this **duality**. They acknowledge privacy as a right and grant citizens new tools of control, yet they leave broad leeways for the state – an uneasy compromise.

This **report has traced that tension through law and case vignettes**. The evidence suggests that without vigilant oversight and proactive measures, the Act's protections will be **asymmetrical**. However, the law also provides a **foundation**: it is, for the first time, a statutory recognition that personal data must be respected in a democracy. If India can implement the DPDP Act as intended – bolstering data stewardship by companies, fostering transparency, and demanding accountability from the state – then the **country can harness digital technology without sacrificing the individual freedoms at the core of its Constitution**.

Ultimately, **privacy and democracy are mutually reinforcing**. A truly democratic India must empower its citizens with knowledge and control over their digital selves. *As Justice Srikrishna has argued, unless privacy is protected, "Indian democracy [will] carry on without its soul."* The **way forward lies in hardening the DPDP framework** where it is soft (independent oversight, citizen remedies), **closing its loopholes** (tightening exemptions, ensuring transparency), and **embedding data rights into India's broader ethos**. With these **reforms**, India can aspire to a **21st-century democracy where welfare and dignity go hand in hand in the digital age**.

REFERENCES

Meltwater (Howe, Sue). "Social Media Statistics for India [Updated 2025]." Meltwater Blog, March 14, 2025. https://www.meltwater.com/en/blog/social-media-statistics-india

Future of Privacy Forum. “The Digital Personal Data Protection Act of India, Explained.” Future of Privacy Forum (blog), October 5, 2023. https://fpf.org/2023/10/05/the-digital-personal-data-protection-act-of-india-explained/

Storyboard18. “Breaking: Govt notifies final DPDP Rules; sets staggered rollout with key obligations for Data Fiduciaries.” Storyboard18, November 14, 2025. https://www.storyboard18.com/digital/breaking-govt-notifies-final-dpdp-rules-sets-staggered-rollout-with-key-obligations-for-data-fiduciaries-84201.htm

Press Trust of India. “Digital Personal Data Protection Rules 2025: Experts warn they grant unchecked power to state.” The News Minute (PTI report), October 14, 2025. https://www.thenewsminute.com/news/data-protection-rules-2025-critics-say-it-grants-unchecked-power-to-the-state

Allu, Vaishnavi. “India’s Digital Inequality: How Far Behind We Really Are in Taking the Internet to the Masses.” The News Minute, October 12, 2016. https://www.thenewsminute.com/news/indias-digital-inequality-how-far-behind-we-really-are-taking-internet-masses-42837

Reporters Without Borders (RSF). “India country page and reports.” RSF, July 2023. https://rsf.org/en/country/india

(NHS / PubMed Central) “Protecting Children’s Data in the Digital Age: Insights from an Instagram Teen Privacy Survey.” PMC (PubMed Central), 2024. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11688589/

The Economic Times. “85.5% of Indian households own a smartphone; 99.5% youth use UPI: MoSPI.” May 30, 2025. https://m.economictimes.com/news/economy/indicators/85-5-indian-households-posses-at-least-one-smartphone-99-5-youth-use-upi-mospi-survey/articleshow/121495764.cms

The Economic Times. “Rural mobile penetration continues to lag.” The Economic Times, October 7, 2025. https://m.economictimes.com/industry/telecom/telecom-news/rural-mobile-penetration-continues-to-lag-report/articleshow/124397844.cms

PRS Legislative Research. A Free and Fair Digital Economy: Report of the Committee of Experts on Data Protection. Committee Report, July 2018. https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018_0.pdf

Gour, Harsh. “Takeaways from the Sanchar Saathi saga: Cybersecurity policy must be evidence-driven, non-arbitrary, transparent.” The Leaflet, December 4, 2025. https://theleaflet.in/digital-rights/law-and-technology/takeaways-from-the-sanchar-saathi-saga-cybersecurity-policy-must-be-evidence-driven-non-arbitrary-transparent/

Abraham, Sarah. “Law & the Digital Society: Fine-tuning Digital Personal Data Protection Rules 2025 for Effective Implementation.” The Hindu Centre, March 3, 2025. https://www.thehinducentre.com/the-arena/current-issues/law-the-digital-society-fine-tuning-digital-personal-data-protection-rules-2025-for-effective-implementation/article69284580.ece

Barik, Soumyarendra. “Centre notifies data protection rules, paves way for India’s first privacy law.” The Indian Express, November 15, 2025. https://indianexpress.com/article/business/centre-notifies-data-protection-rules-paving-way-for-indias-first-privacy-law-10365324/

Burman, Anirudh. Understanding India’s New Data Protection Law. Carnegie Endowment for International Peace (Working Paper), October 3, 2023. https://carnegie-production-assets.s3.amazonaws.com/static/files/Understanding_Indias_New_Data_Protection_Law-3.pdf

Commission Nationale de l’Informatique et des Libertés (CNIL). “Cookies and advertisements inserted between emails: GOOGLE fined €325 million by the CNIL.” Press release, September 3, 2025. https://www.cnil.fr/en/cookies-and-advertisements-inserted-between-emails-google-fined-325-million-euros-cnil

Commission Nationale de l’Informatique et des Libertés (CNIL). “The Korean Data Protection Authority (PIPC) publishes guidelines for foreign companies.” CNIL (France), July 24, 2024. https://www.cnil.fr/en/korean-data-protection-authority-pipc-publishes-guidelines-foreign-companies

Smalley, Suzanne. “South Korean authorities fine Meta $15.6 million for sharing user data.” The Record, November 5, 2024. https://therecord.media/facebook-south-korea-privacy-regulator-fine

DataReportal. Digital 2025: India. DataReportal / Hootsuite & We Are Social, January 2025. https://datareportal.com/reports/digital-2025-india

India, Ministry of Electronics and Information Technology. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023, 11 August 2023). The Gazette of India, August 11, 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

India, Ministry of Electronics and Information Technology. Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 November 2025). The Gazette of India, November 13, 2025. https://dpdpa.com/DPDP_Rules_2025_English_only.pdf

India, Ministry of Electronics and Information Technology. Report of the Committee of Experts on a Data Protection Framework for India. (Chair: Justice B.N. Srikrishna), July 27, 2018. Government of India. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

India, Parliament. Information Technology Act, 2000 (Act No. 21 of 2000, 9 June 2000). Government of India. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

India, Supreme Court. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. https://www.scobserver.in/wp-content/uploads/2021/10/1-266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf

Human Dignity Trust. "Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.: A Landmark Judgment on the Right to Privacy." Full judgment PDF, 2017. https://www.humandignitytrust.org/wp-content/uploads/resources/Puttaswamy-v.-Union-of-India-full-judgment.pdf

Internet Freedom Foundation. "IFF's Initial Statement on the Notification of the Digital Personal Data Protection Rules, 2025." Internet Freedom Foundation (blog), November 14, 2025. https://internetfreedom.in/iffs-initial-statement-on-the-notification-of-the-digital-data-protection-rules-2025/

Internet Freedom Foundation. "Your personal data, their political campaign? How India's elections are data-fueled." July 2024. https://internetfreedom.in/personal-data-political-campaigning/

Kamath, Aaron, and Palak Kapoor. "Global Businesses Should Brace Themselves for India's New Personal Data Protection Law." Business Law Today (American Bar Association, Asia-Pacific section), May 15, 2025. https://www.americanbar.org/groups/business_law/resources/business-law-today/2025-may/india-data-protection-law/

Motiwala, Abdullah Zubair. "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India." SSRN, July 14, 2025. https://ssrn.com/abstract=5335388

NITI Aayog. Data Empowerment and Protection Architecture (DEPA): Executive Summary. New Delhi: NITI Aayog, September 2020. https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Executive-Summary.pdf

NITI Aayog. Online Safety for Children: Protecting the Next Generation from Harm. June 2025. https://niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf

Personal Information Protection Commission (PIPC), South Korea. "PIPC Releases 'Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators'." Press Release, April 12, 2024. https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2488

Saini, Neha. "India's first full-fledged privacy law goes live: What DPDP Rules 2025 mean for your daily apps." Times of India, November 18, 2025. https://timesofindia.indiatimes.com/technology/tech-news/indias-first-full-fledged-privacy-law-goes-live-what-dpdp-rules-2025-mean-for-your-daily-apps/articleshow/125379900.cms

"Govt notifies rules for DPDP Act, putting India's first digital privacy law into effect." The New Indian Express, TNIE Online Desk, November 14, 2025.

https://www.newindianexpress.com/business/2025/Nov/14/govt-notifies-rules-for-dpdp-act-putting-indias-first-digital-privacy-law-into-effect

The Wire Staff. "'Unchecked Powers to Govt, New Barriers to Transparency': IFF on Digital Personal Data Protection Act." The Wire, November 15, 2025. https://thewire.in/rights/unchecked-powers-to-govt-new-barriers-to-transparency-iff-on-digital-personal-data-protection-act

Kantar IMRB & Internet and Mobile Association of India (IAMAI). Internet in India 2024 – Key Highlights. IAMAI report, February 2024. https://www.iamai.in/sites/default/files/research/Kantar_%20IAMAI%20report_2024_.pdf

TheSecretariat.in. "India's Caste Census: A Game Changer for Delimitation and Reservation." July 2024. https://thesecretariat.in/article/registrar-general-s-term-extended-census-in-2025-what-it-means-for-india/

NLS Forum / Socio-Legal commentary. "Caste Data, Digitisation and its Problematic Impact on Privacy and Policing". https://forum.nls.ac.in/slr-forum-blog/caste-data-digitisation-and-its-problematic-impact-on-privacy-and-policing/

SSRN analysis on India/privacy issues : https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4666389_code2043490.pdf?abstractid=4666389

Bhalla, Vineet. "Retired judges hail Centre's recall of order to pre-install cyber app on phones." The Indian Express, December 4, 2025. https://indianexpress.com/article/india/judges-behind-privacy-verdict-hail-recall-of-sanchar-saathi-app-order-flag-issues-10401046/