International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Balancing Innovation and Privacy: A Critical Examination of the Digital Personal Data Protection Rules, 2025 in India

Karthika A

Research Scholar, Law, St Joseph University Tamilnadu

Abstract

The DPDP Rules, 2025, provide detailed procedural criteria for data fiduciaries, such as websites, online services, and social media platforms, in order to put India's Digital Personal Data Protection Act, 2023, into effect. "By laying out procedures for notice and consent, retention and erasure regimes, protections for cross-border data transfers, deadlines for breach notifications, and the institutional framework of the Data Protection Board (DPBI), the Rules expect to increase user agency and responsibility in India's digital ecosystem. Websites and social media platforms are subject to both practical and constitutional implications, and this research paper examines both in detail. The paper synthesises pertinent Indian and comparative case law and situates the Rules within India's current framework for content control and intermediaries, particularly the Information Technology Rules. Here we take a look at how different doctrinal instruments—frameworks for adequacy and transfer, fundamental rights balancing, expectation of privacy, and proportionality—are likely to be used by Indian courts and regulators. This paper argues that although the DPDP Rules are a big improvement over the IT Rules when it comes to data governance, there will still be conflicts between the DPDP's minimization principle and state exemptions, privacy protections and compliance costs, and innovation and compliance." To resolve these issues, the paper suggests early harmonisation measures, clear judicial oversight, and targeted institutional capacity building.

Keywords: Digital Personal Data Protection Rules, Data Fiduciaries, Online Platforms, Right to Privacy, Proportionality Principle, Data Governance in India

Introduction

The digital ecosystem in India generates and manages massive amounts of unique data. This ecosystem encompasses e-commerce platforms, websites, operations, and social media. Although it relied on delegated law to provide practical explanation, the DPDP Act 2023 authorized the framework for data security regulation. "These procedural details and nonsupervisory pathways for data providers were announced on November 14, 2025, by the Ministry of Electronics & Information Technology (MeitY) as the Digital Personal Data Protection Rules, 2025 (DPDP Rules).[1]. The IT Rules, 2021 intersect with an existing, robust central government to prescribe procedures for handling grievances, removing content,

[1] Melissa cyrill , *Digital Personal Data Protection Rules, 2025*, INDIA BRIEFING (Nov. 14 2025) Digital Personal Data Protection Rules, 2025 (India), Notified Nov. 14, 2025 (Ministry of Electronics & Information Technology)

and, in some cases, duties related to traceability. By working together, these administrations pose challenges to conservative legal interpretation, executive direction, and implicit judicial action, which has both positive and negative outcomes. Using a framework of international law and practice, this article analyses the DPDP Rules' wording, explains how they influence online spaces, and situates the Indian approach.

Foundational Elements of India's DPDP Regulatory Framework, 2025

A. Territorial and Material Scope

The Rules establish a geographical nexus for international companies that provide products or services to Indians and apply to all data fiduciaries handling the personal data of Indian data principals.[2] Due to their wide reach, the majority of foreign sites that have Indian users must abide by DPDP requirements."[3]

B. Notice, Consent and Consent Managers

The DPDP Rules emphasize plain-language disclosure, mandate explicit and granular permission, and provide precise notification content (types of data, processing purposes, retention, and data principle rights).[4] "The registration/standards structure for consent managers third-party organizations that can centralize consent acquisition and revocation among fiduciaries is a notable innovation.[5] Consent managers, according to supporters, will empower users and standardize consent channels; detractors caution about potential concentration dangers, UX friction, and integration difficulty.

C. Purpose Limitation, Retention and Erasure

The Rules stress the importance of purpose limitation and require fiduciaries to retain data only as needed. When a certain data class's declared purpose expires, the Guidelines specify the maximum retention period and recommend erasing the data from certain websites and social media platforms. These restrictions will require technology solutions for data-lifecycle management and archiving for user-generated content platforms and analytics apps that rely on historical datasets.[6]

D. Cross-Border Transfers

Transfers across international borders are allowed, but only with certain safeguards and documentation showing that there are equivalent protections outside or through authorized transfer routes. This approach differs from earlier Indian recommendations that skewed toward strict localization, even if the Rules still require careful contractual and organizational safeguards for transfers abroad."[7]

E. Breach Notification and Security

After a breach, fiduciaries are required to put in place "reasonable security safeguards" (encryption, access limits, masking, and logging) and promptly notify the DPBI and impacted principals, including specific

[2] Ibid 2
[3] India strengthens privacy law with new data collection rules, REUTERS, (Nov. 15, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/india--strengthens-privacy-law--with-new-data-collection-rules-2025-11-14/
[4] Ibid 2
[5] Bindu Janardhanan & Scott Warren, *"The Impact of India's New Digital Personal Data Protection Rules,"* PRIVACYWORLD (Apr. 29, 2025), https://www.privacyworld.blog//2025/04/the-impact-of-indias-new-digital-personal-data-protection-rules/
[6] Ibid 2
[7] Melissa cyrill , *Digital Personal Data Protection Rules, 2025*, INDIA BRIEFING (Nov. 14 2025) Digital Personal Data Protection Rules, 2025 (India), Notified Nov. 14, 2025 (Ministry of Electronics & Information Technology)

information in such communications. Although the Rules permit some contextuality, practice notes suggest a 72-hour window for initial reporting in some duty matrices distributed to industry.[8]

F. DPBI Powers and Enforcement

"The Rules operationalise complaint procedures, adjudicatory timelines and penalty mechanics through the DPBI. Effective enforcement will depend on DPBI's resourcing, technical expertise, and procedural safeguards to ensure independence and promptness.

Operational Impact of the DPDP Rules on Websites and Social Media Platforms

Agreement and User Experience Design Instead of vague, long-form policies, platform consent flows should include clear, actionable prompts tailored to the precise goal. When utilizing consent managers, platforms are required to provide standardized consent tokens and incorporate APIs. This overhaul is challenging for legacy platforms and requires coordination between technical, legal, and product teams.[9]

G. Product Features vs. Data Minimization

Ad targeting, recommendation algorithms, and customized feeds are just a few product features that rely on massive amounts of historical data. Under the DPDP, platforms must either obtain express agreement for processing personal data or adapt their functionality to rely on less personal data, anonymized signals, or on-device processing. Strategies such as differential privacy and federated learning may be required, or the reach of behavioral advertising may be restricted."[10]

AI Training Sets, Retention, and Archival

Retention minimization and model performance must be balanced by social media platforms that use past data for machine learning model training. The Rules call for meticulous documenting of the legal justifications for keeping data for model training, as well as potentially novel approaches (synthetic data, aggregated models) to limit the use of identity data. The DPDP Rules' implications for AI training are highlighted in SSRANA opinion, which also emphasizes the potential restrictions on the unapproved use of personal data for training.[11]

A. International Architectures and Localization Decisions

Even if the Rules permit transfers with protections, many companies may still choose to host or process personal data of Indian residents in data centers in India to reduce regulatory compliance costs and respond faster to regulatory or law enforcement demands. Increasing both capital and operating expenses, this trend enhances regulatory certainty.

B. Public Reporting and Incident Response

Platforms must implement systems for forensics, detection, and legal reporting in order to comply with breach-notification regulations. Public disclosure in a timely manner may influence reputational risk and prompt authorities to take enforcement action in cases where reporting is inadequate. There has been an uptick in the market's focus on rapid breach response, according to press reports and industry advice.[12]

---

[8] Vikrant rana and et al., *meity notifies final digital personal data protection rules 2025*, SSRANA , (Nov. 14 2025), https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/

[9] Transforming data privacy: DPDP Rules, 2025, EY INDIA, (28 Jan 2025), https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025

[10] Supra 5.

[11] Supra 8

[12] *Dpdp rules-2025-rules explained as they come into effect what they mean for you*, TIMES OF INDI A,(nov 14, 2025), https://timesofindia.indiatimes.com/technology/tech-newss/dpdp-rules-2025-rules-explained-as-they-come-into-effect-what-they-mean-for-you/articleshow/125325252.cms

Judicial Foundations and Emerging Litigation under India's Data Protection Regime

A robust understanding of likely legal challenges requires a survey of key Indian precedent:-

- ***Justice K.S. Puttaswamy (Retd.) v. Union of India***

In Puttaswamy, the SC established a three-part proportionality test (lawfulness, need, and proportionality) for state intrusions and acknowledged a basic right to privacy under Articles 14, 19, and 21. This case will influence judicial evaluation of DPDP Rule provisions that allow state access or security exemptions, as well as provide insight into the requirements for traceability and retention.[13]

- ***Shreya Singhal v. Union of India*** [14]

The Singhal emphasized that interposers should not be burdened with burdensome takedown liabilities in the absence of court orders or legal guidance and declared Section 66A of the IT Act to be unconstitutional due to its overbreadth. The ruling emphasizes due process conditions for content junking and central impunity while limiting governmental overreach.

- ***Anuradha Bhasin v. Union of India*** [15]

The Bhasin created a proportionality frame for internet shutdowns, strengthening severe procedural safeguards for limitations on digital dispatches, indeed though it is not a data- protection case per se. Its sense is applied to sequestration and data- access challenges where internet rights are impeded by government directives.

Comparative Law Analysis of Data Protection: India's DPDP Rules, 2025 in Global Perspective

- **Importance of Comparative Data Protection Law**

The sheer essence of data protection legislation makes it global. Digital platforms, websites, and social media intermediaries often operate across states, and personal data often moves across borders as well. Consequently, local constitutional standards and internationally acknowledged privacy regimes must be considered while assessing the efficacy and legitimacy of DPDP Rules, 2025. By looking to comparative law for guidance, Indian courts and regulators can find solutions to conflicts including privacy, free speech, governmental surveillance, and corporate interests.

- **European Union: Rights-Centric and Proportionality-Driven Model**

A. Data Security as an Essential Right

The EU considers data protection to be a fundamental right, as stated in Article 8 of the EU Charter of Basic Rights.The EU framework differs from many other states due to this constitutional elevation. The General Data Protection Regulation (GDPR), which sets strict standards on data controllers and enforceable rights for data subjects, operationalises this right.[16] Although they range in intensity, India's DPDP Rules, are structurally similar to this rights-based method. The Data Protection Board (DPBI) is responsible for enforcing the DPDP Act's recognition of individual rights to access, correction, and

[13] Justice K.S. Puttasswamy (Retd.) v. Union of India, (2017) 10 SCC 1 https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/43.pdf?utm_

[14] Shreya Singhal v. Union of India (2015) is AIR 2015 SC 1523, https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/06/Shreya_Singhal_vs_U.O.I_on_24_March_2015.pdf?utm_

[15] Anuradha bhasin v. Union of india (2020) 3 SCC 637, https://api.scii.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf?utm_

[16] Charter of Fundamental Rights of the European Union art. 8, 2012 O.J. (C 326) 391, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

erasure, as opposed to independent supervisory institutions with extensive investigative authority, as is the case in the EU.[17]

B. Lawful Bases of Processing and Consent

Consent is just one of several legitimate grounds for data processing under Article 6 of the GDPR, including public interest, legal requirements, and legitimate interests.[18] With this pluralistic framework, responsibility is maintained while flexibility is allowed. However, with only a handful of "legitimate uses," consent-based processing is the backbone of India's DPDP Rules." According to comparative research, genuine autonomy can be compromised and consent fatigue can be caused by an over-reliance on consent.Therefore, the EU model offers a revealing comparison by finding a middle ground between user rights and practical feasibility.[19]

C. Right to Erasure: The Google Spain Doctrine

In Google Spain SL v. Agencia Española de Proteção de Datos (AEPD), the Court of Justice of the European Union recognised the "right to be forgotten," which permits anybody to ask for their personal data to be deleted from search results in certain situations. Importantly, the Court stressed finding a harmony between the public interest, the right to speech, and privacy.Although erasure rights are provided, a balancing criterion is not specifically codified in India's DPDP Rules. Therefore, when resolving disputes between erasure demands and Article 19(1)(a) constitutional free speech guarantees, Indian courts are likely to consult Google Spain. [20]

D. Cross-Border Transfers and Schrems II

The EU's rigorous attitude to international data transfers was strengthened in Schrems II, when the CJEU invalidated the EU-US Privacy Protection for failing to provide effective protection against US surveillance laws.[21] The court's ruling states that exporters must ensure "essentially equivalent" protection in the receiving country. However, there is no exhaustive adequacy criterion specified in India's DPDP Rules, which permit cross-border transfers subject to government-approved safeguards. If foreign monitoring regimes undermine the constitutional privacy protections acknowledged in Puttaswamy, comparative research suggests that Indian courts may need further procedural protections in the future.[22]

- **United States: Sectoral Privacy and Constitutional Restraints**

A. Fragmented Statutory Framework

The US lacks a comprehensive federal data protection act. Instead, privacy regulations are industry-specific (e.g., HIPAA, COPPA, GLBA) and complemented by state legislation like the California Consumer Privacy Act (CCPA)[23]. This contrasts with India's unified DPDP system. Scholars argue that

[17] Digital Personal Data Protection Act, 2023 (India), https://www.meity.gov.in/data-protection-framework
[18] Regulation (EU) 2016/679, General Data Protection Regulation art. 6, https://eur-lex.europa.eu/eli/reg/2016/679/oj
[19] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013), https://harvardlawreview.org/print/vol-126/privacy-self-management-and-the-consent-dilemma/
[20] Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131
[21] Data Protection Comm'r v. Facebook Ireland Ltd (Schrems II), Case C-311/18, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311
[22] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[23] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199,https://oag.ca.gov/privacy/ccpa

the US approach prioritizes innovation and free markets over privacy concerns. In contrast, India's DPDP Rules aim for thorough regulation.[24]

B. Reasonable Expectation of Privacy: *Carpenter v. United States*

In ***Carpenter v. United States***, the U.S. SC held that According to the Fourth Amendment, long-term access to cell-site location data is a search that needs a warrant.[25] The Court rejected a rigid application of the third-party doctrine in the digital age.

This reasoning is highly relevant to India, where traceability and metadata retention obligations under intermediary regulations may intrude upon informational privacy. Indian courts may find Carpenter persuasive when evaluating proportionality and necessity under Article 21, as articulated in Puttaswamy.

C. Surveillance and Judicial Oversight

The United States jurisprudence increasingly emphasizes judicial oversight for digital monitoring. However, India's DPDP Rules offer extensive state exemptions for sovereignty and public order in the absence of clear warrant requirements. According to comparative constitutionalism, Indian courts may include procedural safeguards in the Rules to ensure constitutional validity.

- **United Kingdom: Continuity After Brexit**

After Brexit, the United Kingdom maintained GDPR principles in the UK GDPR and the Data Protection Act of 2018.[26] The United Kingdom's system exemplifies how the Information Commissioner's Office (ICO) can exercise impartial oversight while still allowing for national security exemptions. When it comes to institutional design and accountability, the UK model is relevant because India's DPDP system does not have an equivalent independent supervisory authority.

- **Asia-Pacific Approaches**

Singapore: Business-Friendly Consent Model- Singapore's Personal Data Protection Act (PDPA) prioritizes permission but allows for implied consent in some business circumstances, lowering compliance obligations. Singapore places a higher value on regulatory efficiency and innovation than India's tighter permission system.

China: State-centric control.- China's Personal Information Protection Law (PIPL) combines robust individual rights with broad governmental control and data localization requirements.[27] India's DPDP Rules fall somewhere in the center, being less intrusive than China's but more state-centric than the EU's.

Comparative Jurisprudential Insights for India's Data Protection Regime

A comparative analysis shows various normative lessons:-

- Balancing Tests Are Essential: Courts in the EU and the US routinely balance privacy against conflicting interests. India must achieve equal conceptual clarity.
- Judicial Oversight of State Access: Comparative regimes emphasize warrants or independent review, which is lacking in India's DPDP Rules.

[24] Paul M. Schwarrtz & Daniel J. Solove, Information Privacy Law (6th ed. 2021), https://aspenpublishing.com/products/solove-information-privacy-law

[25] Carpenter v. United States, 585 U.S.(2018),https:.//www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

[26] Data Protection Act, 2018 (UK), https://www.legislation.gov.uk/ukpga/2018/12/ contents

[27] Personal Information Protection Law of the People's Republic of China (2021), https://.digichina.stanford.edu/work/translation-personal-information--protection-law-of-the-peoples-republic-of-china/

- Cross-Border Adequacy Standards: Schrems II emphasizes the need for a thorough examination of foreign monitoring regimes. Deletion and takedown rights must be balanced with free expression protections, as illustrated by Google Spain and Shreya Singhal.

The DPDP Rules, 2025 in India are a hybrid data protection architecture, according to the comparative research. It takes elements from the EU's rights-based conceptions, global jurisprudence's constitutional privacy reasoning, and the regulatory flexibility of Asia-Pacific regimes. But issues like judicial oversight, cross-border transfers, and state exemptions remain unresolved, which could lead to the need for interpretational intervention by Indian courts. The trajectory of India's cyber privacy legislation is heavily dependent on comparative law.

Tensions, Trade-offs and Practical Consequences

A. Traceability v. Privacy

In practice, traceability orders (for originator identification) will run into DPDP's minimisation duty. Platforms may be forced to retain persistent identifiers for potential future orders a practice contrary to minimisation and purpose limitation. Judicial balancing will be necessary, and administrative guidelines clarifying narrow circumstances for traceability could reduce litigation.[28]

B. State Exemptions and Oversight

The DPDP framework contains exemptions for state processing on reasons like public safety, security, and integrity. Puttaswamy's proportionality test requires that such exemptions be narrowly construed, accompanied by procedural safeguards (e.g., independent judicial oversight, necessity demonstration, and contemporaneous record-keeping).[29]

C. Compliance Costs and Innovation

Smaller websites and start-ups have higher compliance costs, including data inventories, consent engineering, breach response, and possible localisation. Without transitional assistance or tiered requirements, enforcement may cement incumbents and raise entry barriers, decreasing competitive dynamism.[30]

D. Research, Journalism, and Public Interest Uses.

Strict privacy and retention policies can impede investigative journalism and studies that rely on personal information. Carefully drafted exemptions (restricted, time-limited, audit-trail based) for public interest processing could meet these concerns while protecting privacy.

Recommendations

- Harmonize DPDP and IT Rules using collaborative guidelines from MeitY and law enforcement agencies to eliminate operational conflicts (traceability restrictions, retention harmonization).
- Limit state exclusions and demand prior judicial authority for intrusive access, save in narrowly defined situations; and mandate transparency reporting on all government access.
- Phased compliance and technical assistance for SMEs includes standardised toolkits, free consent manager SDKs, and compliance roadmaps.

[28] Vikrant rana and et al., IT Rules Amendment: Regulating Synthetically Generated Information In India's AI And Privacy Landscape, SSRANA, (31 Dec 2025) https://www.mondaq.com/india/new-technology/1725598/2025-it-rules-amendment-regulating-synthetically-generated-information-in-indias-ai-and-privacy-landscape?utm_

[29] Supra 14

[30] Transforming data privacy: DPDP Rules, 2025, EY INDIA, (28 Jan 2025), https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025

- DPBI independence and technical capacity: establish transparent nomination processes, technical panels, and expedited appellate pathways.
- Carve-outs for journalism and research with safeguards, such as data minimization and oversight to protect public interest activity.

Conclusion

A rights-based, procedurally-based framework for data governance in India is established under the DPDP Rules of 2025. Particularly in the areas of consent engineering, retention regulations, breach reporting, and cross-border compliance, the Rules necessitate operational redesigns of online platforms and websites. By following regulatory guidelines and judicial interpretations informed by constitutional law (Puttaswamy, Singhal, Anuradha Bhasin) and compelling comparative precedents (Google Spain, Schrems II, Carpenter), the key legal disputes surrounding traceability vs. minimization, state exemptions vs. privacy, and enforcement costs vs. innovation will be resolved. If India's data privacy regime is successful in its aims to safeguard personal freedom and encourage a healthy, conscientious online community, it will be because of its solid institutional architecture and effective harmonisation.

Bibliography

1. "Anuradha bhasin v. Union of india (2020) 3 SCC 637, https://api.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf?utm_
2. Data Protection Act, 2018 (UK), https://www.legislation.gov.uk/ukpga/2018/12/contents
3. Data Protection Comm'r v. Facebook Ireland Ltd (Schrems II), Case C-311/18, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311
4. Digital Personal Data Protection Act, 2023 (India), https://www.meity.gov.in/data-protection-framework"
5. Bindu Janardhanan & Scott Warren, *"The Impact of India's New Digital Personal Data Protection Rules,"* PRIVACYWORLD (Apr. 29, 2025), https://www.privacyworld.blog/2025/04/the-impact-of-indias-new-digital-personal-data-protection-rules/
6. "California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199,https://oag.ca.gov/privacy/ccpa
7. Carpenter v. United States, 585 U.S.(2018),https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf
8. Charter of Fundamental Rights of the European Union art. 8, 2012 O.J. (C 326) 391,
9. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013),https://harvardlawreview.org/print/vol-126/privacy-self-management-and-the-consent-dilemma/
10. *Dpdp rules-2025-rules explained as they come into effect what they mean for you*, TIMES OF INDIA,(nov 14, 2025), https://timesofindia.indiatimes.com/technology/tech-news/dpdp-rules-2025-rules-explained-as-they-come-into-effect-what-they-mean-for-you/articleshow/125325252.cms
11. Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12,
12. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT
13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

14. India strengthens privacy law with new data collection rules, REUTERS, (Nov. 15, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/india-strengthens-privacy-law-with-new-data-collection-rules-2025-11-14/
15. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1
16. Melissa cyrill , *Digital Personal Data Protection Rules, 2025*, INDIA BRIEFING (Nov. 14 2025) Digital Personal Data Protection Rules, 2025 (India), Notified Nov. 14, 2025 (Ministry of Electronics & Information Technology)
17. Paul M. Schwartz & Daniel J. Solove, Information Privacy Law (6th ed. 2021), https://aspenpublishing.com/products/solove-information-privacy-law
18. Personal Data Protection Act 2012 (Singapore), https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation
19. Personal Information Protection Law of the People's Republic of China (2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china/
20. Regulation (EU) 2016/679, General Data Protection Regulation art. 6, https://eur-lex.europa.eu/eli/reg/2016/679/oj
21. Shreya Singhal v. Union of India (2015) is AIR 2015 SC 1523, https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/06/Shreya_Singhal_vs_U.O.I_on_24_March_2015.pdf?utm_
22. Vikrant rana, Anuradha Gandhi nand Prateek Chandgothia, *meity notifies final digital personal data protection rules 2025*, SSRANA , (Nov. 14 2025)," https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/