



Gokhale Education Society's

Swayamprakash

Luminescence

Peer-reviewed Journal of Research

Multidisciplinary

**Prin. T. A. Kulkarni Vidyanagar, College Road, Nashik - 422 005,
Maharashtra, India. Tel. : (0253) 2572520 Fax : (0253) 2578832**

**JOURNAL OF
RESEARCH**

ISSN : 2249 - 9016

October : 2025

Volume : VIII, Issue : III

*IN THIS ISSUE***Women Empowerment through Rights Based Approach : A Case Study of MASUM's Intervention**

- Waghmare S. A.* 794

Justice Delayed, Justice Denied: Legal Challenges in Gender-Based Violence Cases

- Shetye S.*, Negi S.** 800

Image Based Sexual Abuse and the Limits of Territorial Jurisdiction over Foreign Based Servers

- Agrawal S.* 814

The Empowered Mind : Navigating Psychological Barriers to Women's Empowerment

- Surywanashi. Y.*, Mane J.** 826

The Concept and Practice of Gender Justice in India

- Bhat P. I.* 832

Empowering Women in Goa's Unorganized Sector through the Goa State Migrant Worker Cell and Intervention Strategies by Disha Foundation

- Borhade A.,* Dey S.,** Jain I.,*** Kundaikar V.,**** Vaingankar N.,***** Dessai D. P.***** 856

Women's Portrayal: Modern Misconceptions Versus Ancient Dharma

- Gharote A.* 867

Honour Killings - A Tragic Reality in Socio-Legal Context Violating Human Rights

- Gupta L.,* Bala M.** 879

From Vulnerability to Empowerment: The Role of Data Localisation in Safeguarding Women's Digital Rights in India

- Shetty V. 891

From Vulnerability to Empowerment : The Role of Data Localisation in Safeguarding Women's Digital Rights in India

- Shetty V.*

*Research Scholar, MCE Society's A. K. K. New Law Academy, Pune

Data has emerged as a new currency in the rapidly developing digital age which is strong, individualised and vulnerable to abuse. The digital revolution has unlocked unprecedented opportunities for women in areas such as civic engagement, entrepreneurship and education however, it has also introduced complex challenges that disproportionately impact them particularly in relation to data security. "Cyber stalking", identity theft, blackmail and reputational damage are all common outcomes of the exploitation of women's personal data which is regularly taken from social media, health applications, financial tools and professional platforms. These challenges are further compounded when women's sensitive data is stored in foreign jurisdictions, limiting the efficacy of domestic legal remedies and regulatory enforcement. This paper critically examines the gendered vulnerabilities associated with digital data exposure based on Indian legal statutes such as the "Information Technology Act, 2000" and the "Digital Personal Data Protection Act, 2023". It places particular emphasis on the emerging role of data localisation laws, which seek to ensure that critical personal data remains within India's sovereign control. Data localisation promotes enforcement of data protection standards, improves regulatory monitoring and expedites the resolution of complaints by maintaining data inside national borders especially for women harmed by digital technology. **Incorporating** international frameworks and gender responsive policy insights the study highlights significant enforcement shortcomings limited digital literacy and structural barriers within existing data governance systems. By positioning digital security and data sovereignty as foundational to the protection of women's rights in the contemporary digital environment the paper proposes a comprehensive model that enables women to engage with the online world with greater autonomy respect and legal assurance.

Key Words : Data Localisation, Women's Digital Rights, Cyber security and Gender, "Digital Personal Data Protection Act, 2023", Gender-Sensitive Data Governance.

Introduction : Safeguarding Women's Digital Rights in India's Data Landscape

With more than 800 million internet users propelling social and economic changes, India's digital revolution has brought about previously unheard-of levels of connectedness. Programs like Digital India, which expand access to online education, e-commerce, and governance platforms, are driving a surge in women's involvement in this digital ecosystem. Though gender disparities in adoption and skill sets still exist, similar patterns around the world demonstrate how digitization empowers women through remote labor,

financial inclusion, and political participation.¹ Although women's digital participation has increased by 50% in India in recent years, complete equity is still constrained by factors including cost and cultural norms.² Personal data, sometimes referred to as the "new oil" because of its importance in enabling algorithms, tailored services, and innovation, is at the core of this digital economy. Personal data generates trillions of dollars in worldwide value by enabling tailored experiences in social networking, healthcare, and e-commerce. Its commodification, however, presents serious issues since, in the absence of sufficient protections, data collection methods may be exploited.³

In the digital sphere, where identity theft, blackmail, cyber stalking, and reputational harm are common, women are particularly vulnerable due to their gender. According to estimates, these incidences have increased significantly in India, where women make up over 60% of victims of cybercrime, which frequently involves doxxing or modified photos that reinforce harassment and social stigma.⁴ In addition to violating privacy, these threats discourage women from participating online, which exacerbates gender inequality. These concerns are increased when women's data is stored in foreign jurisdictions, since timely access for investigations is hampered by inconsistent legal standards and jurisdictional barriers. Data stored overseas may be more vulnerable to breaches that result in identity theft or targeted abuse due to less privacy regulations or foreign surveillance.⁵ Cross-border data flows, for example, may prolong victims' vulnerability by delaying Indian law enforcement's response to complaints.⁶

By requiring storage within India, enabling speedier regulatory control, and lowering need on foreign collaboration, data localisation shows promise as a protection for women's digital rights. It can strengthen data sovereignty by guaranteeing that private data, such as location or health information, which are frequently more important for women, is shielded from unwanted foreign access.⁷ In the context of India's changing legal system, Foundational safeguards against cybercrimes are provided by the "Information Technology Act, 2000" (IT Act), which includes Sections 66A (now struck down but still significant) and 66C on identity theft, which addresses online harassment.⁸ Although it does not specifically address gender related issues, the "Digital Personal Data Protection Act, 2023" (DPDP Act) expands on this by instituting consent-based data processing, deletion rights, and monitoring through a Data Protection Board.⁹

Is it possible for data localisation to improve online enforcement and protection of women's rights? Advocates contend that it strengthens local jurisdiction, preventing abuses like extortion and facilitating quicker recourse under the DPDP Act.¹⁰ However, detractors caution about the dangers of government overreach that could violate privacy, higher expenses, and possible stifling of innovation.¹¹ Ultimately, balanced implementation could empower women, aligning data policies with equity in India's digital future.

Gendered Vulnerabilities in the Digital Space

The convergence of digital life and patriarchal authority is reflected in gendered vulnerabilities in the digital sphere. In addition to being users, women also perceive technology as targets, whose identities, bodies, and reputations are mediated by databases and platforms. Although many of these damages are explicitly recognized

by Indian law, survivors frequently experience prolonged exposure and secondary victimization as a result of enforcement loopholes, sluggish takedowns, and cross-border data transfers. Among the various manifestations of digital exploitation are cyberstalking and online harassment, both of which entail sustained, intrusive surveillance or contact that undermines an individual's ability to speak freely and move without fear. Even before the criminal law transition in 2024, stalking was particularly addressed under Indian penal law, and courts have interpreted internet harassment through constitutional lenses that protect expression and dignity.¹² Identity theft and impersonation are prosecuted under the "Information Technology Act, 2000" (IT Act), which penalizes identity theft and cheating by personation utilizing computer resources. This includes using stolen photographs, Aadhaar-linked details, or SIM-based OTPs to build phony profiles or swindle. The regulations pertaining to sexually explicit content and obscenity are implicated by non-consensual intimate imagery (NCII) and "revenge porn," with intermediaries being required to remove such content.¹³ The Supreme Court has dealt with this dynamic when directing proactive suppression of illegal results. Blackmail, doxxing, or cyber bullying and threats frequently combine these vectors to cause reputational injury that persists in search indices even after removal.¹⁴

Social media (profile scraping; location metadata), health apps (menstrual and fertility logs), banking services (KYC repositories), and professional platforms (resume boards; messaging integrations) are some of the data sources that put women at risk. In addition to breaches, inference is the issue since machine readable trails can be used to forecast private information. Whether collected and shared by private or public entities, the constitutional right to privacy, which is upheld as fundamental to autonomy and dignity requires need and proportionality.¹⁵ Intermediary due diligence requirements require the use of grievance officers, time-bound content removal, and traceability for specific violations; however, these compliance tools must be balanced against the rights to free speech and due process.¹⁶

The multi-dimensional harms of cyberstalking and non-consensual intimate imagery (NCII) become evident through impact analysis, as affected women consistently describe experiences of anxiety, hypervigilance, and restrained self-expression. Reputational attacks circulate more rapidly than subsequent corrections, disproportionately affecting women by undermining their social standing and marital prospects. Legally, survivors must contend with jurisdictional complexity, difficulties of proof, and delayed relief, even though there are numerous causes of action (criminal complaint, IT Act reporting, platform grievance, and civil torts including defamation or privacy). Economically, employment and income are negatively impacted by targeted fraud and professional sabotage (impersonation on professional networks; mass-report brigading). The right to access the internet has been characterised as connected with fundamental freedoms, and courts have acknowledged that meaningful digital participation education, employment, and speech requires secure settings in addition to connectivity.¹⁷

The vectors of harm are evident in the following case studies,

Hyderabad Deep Fake Blackmail : A 19-year-old student in Hyderabad filed a

complaint alleging that a man had created a nude deep fake image of her using AI tools and was using it for blackmail. The re-uploading and circulation of the manipulated image mirrors the kind of harm in your scenario. (Reported in the The Times of India).¹⁸

Dibrugarh / Assam Morphed Image Case: In Assam, a man was arrested for distributing altered explicit images (using AI tools) of a woman (his former acquaintance). He superimposed her face onto adult content and shared across platforms. This is a close parallel: repeated distribution, manipulation, and reputational harm. (Reported in the The Times of India.)¹⁹

Persistent harassment of a woman doctor via calls/texts: Lucknow case of a woman doctor receiving **5,000 lewd texts and 1,000 calls in a day**; police registered an FIR. (Reported in Hindustan Times)²⁰

In every instance, centering survivors necessitates immediate steps to secure digital traces (logs, headers, hashes), combined recourse to diverse legal and regulatory mechanisms, and trauma-responsive support, all under a constitutionally compliant enforcement model that balances privacy protections with the right to free expression.²¹

Legal and Regulatory Framework in India

1. The Information Technology Act (IT Act) of 2000

Hacking (Sec. 66), identity theft (Sec. 66C), cheating by computer resources (Sec. 66D), posting private or obscene photographs (Sec. 66E, Sec. 67A), breach of confidentiality (Sec. 72), and cyberterrorism (Sec. 66F) are among the many cybercrimes that are made illegal by the Information Technology Act of 2000.²² In accordance with updated regulations from 2013 and 2022, administrative tools such as the Computer Emergency Response Team (CERT-In) make incident reporting and response easier.²³ Despite its extensive scope, the Act does not contain gender-specific provisions; the IT Act does not specifically address online violence against women, and while general regulations such as the Protection of Sexual Harassment Act, 2013 or POCSO Act, 2012 may be applicable in online settings, enforcement issues persist.²⁴

2. “Digital Personal Data Protection Act, 2023” (DPDP Act)

India’s first national data privacy law is the “Digital Personal Data Protection Act, 2023”, which came into effect on August 11, 2023. It covers digital personal data that is gathered or transferred in digital form, and it also covers data processed outside of India in relation to providing Indian “Data Principals” with products or services.²⁵ The Act mandates free, specific, informed, unconditional, and unambiguous consent for data processing; provides rights to access, correction, erasure, and withdrawal of consent; requires notices in English or any language in the Eighth Schedule; and obliges Data Fiduciaries to implement security safeguards and data breach notifications. Additionally, it creates the Indian Data Protection Board as an adjudicatory body.

But there are still a lot of unanswered questions on issues unique to women. The Act is criticized for its gender-blind framework, which excludes intersectional monitoring that may address issues like gender-based profiling or harassment directed at women, mandated bias audits, and context-aware consent for vulnerable groups.²⁶ The Act’s

ability to effectively address online problems that disproportionately affect women may be limited by this gender-neutral default.

3. Role of Foreign Data Storage - Extraterritorial Challenges

India's legal framework allows for extraterritorial application: the DPDP Act protects data processed abroad when linked to products intended for Indian citizens, and the IT Act (via Sec. 75) can punish crimes committed abroad if they involve Indian networks or systems. However, there are real-world issues with offshore or foreign data storage. Conflicting international laws and jurisdictional constraints make it difficult to pursue data fiduciaries, execute removal orders, or achieve legal recourse when data is hosted outside of India's jurisdiction. This compromises enforceability even in cases when legal power is present.²⁷ Furthermore, the DPDP Act now defers clear legal clarity by leaving such authorities to future notifications, even in the face of discussions about data localisation or restrictions on cross-border transfers.²⁸

Data Localisation as a Tool for Women's Digital Empowerment

Data localization, which mandates that specific data be processed and/or stored on servers in India, lies at the nexus of market regulation, cyber security, privacy, and sovereignty. In India, localisation can be facilitated by a general personal data regulation that regulates outward transfers, sectoral (such as payments), or incident-response driven (such as cyber security logs). Ensuring regulatory and law enforcement access, decreasing cross-border investigative latency, and enhancing responsibility over sensitive personal data including women's data in the contexts of health, finance, safety, and social media, are some of its goals.

There are three specific advantages that localisation can offer for women's digital empowerment. First, by eliminating Mutual Legal Assistance Treaty (MLAT) delays when evidence is located offshore, it might expedite the access to evidence for cases involving cyberstalking, non-consensual imagery ("revenge porn"), doxing, impersonation, and extortion offenses that disproportionately affect women.²⁹ Second, when fraud or coercive financial abuse affects women, sectoral mandates like the Reserve Bank of India's "on-soil" storage for payments data provide regulators with "unfettered supervisory access," enhancing redress. Third, in order to facilitate prompt attribution of harassment accounts and organized trolling, CERT-In's incident-reporting and log-retention guidelines mandate that companies maintain 180-day logs in India.

Localisation can speed up the process from complaint to charge sheet, which is crucial in situations where harms grow rapidly online, but it is not a panacea for underreporting or social stigma. Women's cyber complaints are still empirically significant, and converting complaints into convictions depends on improved evidence pipelines and quicker platform collaboration.

The current framework in India combines selective localisation and transfer control. Following Puttaswamy, the "Digital Personal Data Protection Act, 2023" (DPDPA) recognizes informational privacy and allows cross-border transfers unless restricted jurisdictions are notified by the central government. This is sometimes referred to as a

“whitelist by default” model, and it will be operationalised through future regulations.³⁰ In contrast to localisation, this preserves a policy lever to limit the export of sensitive personal data in situations where enforcement is not feasible or when there is a high risk to rights. In addition, the RBI payments circular requires that end-to-end payment data be stored locally, and CERT-In guidelines require that security logs be localized. These are two important levers in situations involving fraud, abuse, and platform manipulation that impact women.³¹

In the Indian setting, there are actual limitations and critiques. Technically and financially, requiring on-soil storage can increase expenses for women-serving SMEs and civil society organizations, split cloud infrastructures, and limit access to top-notch international security tools. Civil liberties organizations have cautioned that if not well regulated, widely scoped logging and accelerated disclosure powers run the risk of enabling surveillance creep, which would restrict women’s advocacy and speech, particularly in vulnerable communities. Due process is not always ensured by pure localisation; content-blocking under Section 69A of the IT Act may go too far in the absence of adequate notice, openness, and independent supervision.³² Furthermore, localisation cannot replace survivor-centric procedures and protection orders, nor can it resolve police capacity issues, digital forensics, or trial delays on its own.

Therefore, a balanced Indian pathway would:

- (i) maintain the transfer-control lever of the DPDPA with a transparent, rights-based test for limiting destinations;
- (ii) maintain sector-specific localisation paired with interoperability standards for high-risk domains (payments, health, and children’s data);
- (iii) reinforce survivor-centered protocols for platform cooperation and evidence preservation (time-bound disclosure, safe-harbor for trusted flaggers, and dedicated hotlines); and
- (iv) incorporate safeguards; judicial or independent oversight, proportionality assessments, minimized log scopes, and public transparency reports for any state access.

This calibrated strategy, which is based on Puttaswamy’s proportionality and dignity principles, can turn localisation from a brutal tool into a useful tool for women’s digital empowerment.

Structural Barriers and Policy Gaps

The effectiveness of data localisation in safeguarding women’s digital rights in India must be evaluated against persistent structural barriers and policy gaps.

Digital Literacy

Women’s low level of computer literacy is a major problem, especially in underserved and rural areas. Women are frequently ignorant of internet dangers, cyber hygiene, and their legal rights in the event of digital exploitation. Less than one in three Indian internet users are female, according to a UNICEF survey, indicating a clear gender gap in digital

access and expertise.³³

Regulatory Weaknesses

Vulnerability to identity theft, extortion, and cyber stalking is increased by this ignorance. Lack of literacy hinders women's ability to exercise their rights under the Digital Personal Data Protection Act of 2023 and the Information Technology Act of 2000, even if data localisation guarantees safer preservation of personal data.

The data protection laws in India are still disjointed. Although the Digital Personal Data Protection Act of 2023 offers a framework for protecting private information, its effectiveness is diminished by inadequate enforcement, jurisdictional overlaps, and insufficient monitoring.³⁴ Law enforcement organizations frequently lack the necessary expertise and resources to handle gendered cybercrimes. According to an empirical research, women usually face barriers when attempting to file complaints about cybercrime because of inadequate institutional coordination and investigative delays.³⁵

Cultural and Structural Barriers

Lastly, women's ability to exercise their digital rights is further limited by deeply ingrained social and cultural conventions. Male family members continue to mediate many women's access to cell phones and the internet, which restricts their independence.³⁶ Systemic underreporting is a result of women's reluctance to disclose digital violations due to fear of damage to their reputation. According to the National Crime Records Bureau, the number of cybercrimes that target women is much lower than the actual number on the ground.³⁷ Because women might not feel empowered to seek redress, these sociocultural variables diminish the effectiveness of even strong data localisation policies.

To summarize, data localization is a crucial technological and legal protection, to guarantee that Indian women can genuinely benefit from these protections, it is equally important to close the digital literacy gap, bolster regulatory enforcement, and eliminate systemic injustices.

Recommendations and Policy Insights

The role of data localisation in safeguarding women's digital rights in India necessitates multi-pronged policy interventions. Regulatory and Legal Improvements. Although it creates a framework for the control of personal data, the "Digital Personal Data Protection Act, 2023" (DPDP Act) does not include gender-sensitive operational instructions. In order to prevent the misuse of women's data, especially health, financial, and biometric information, stronger enforcement mechanisms must be established through sectoral directives and regulatory laws. Institutional accountability may be improved by the Data Protection Board establishing gender-specific compliance procedures.

Capacity Building Programs for women's digital literacy are still essential. Research indicates that women's ability to seek recourse against cyber abuse is severely hampered by a lack of knowledge about their online rights.³⁸ Gender-inclusive curriculum that emphasize recognizing digital dangers, reporting procedures, and exercising data rights under the DPDP Act should be incorporated into government and civil society activities.

Data localisation integration: For swift access by domestic regulators and courts, a framework for the required localisation of vital women's data such as medical records, police reports, and educational data is necessary. In addition to enhancing investigative capabilities, localisation guarantees quicker grievance resolution in situations involving identity theft or online harassment. To avoid state overreach, these actions should be counterbalanced with sufficient protections.

International Collaboration: India is able to adopt international models best practices. The General Data Protection Regulation (GDPR) of the European Union offers a strong model for cross-border protections and explicit permission requirements.³⁹ In a similar vein, Australia's Privacy Act 1988 provides robust safeguards for private information, providing a model for policies that prioritize women.⁴⁰ India can establish a rights-based, technologically and socially inclusive strategy to data localisation with the help of bilateral and global cooperation. In conclusion, a more gender-sensitive data protection ecosystem may be established in India by enforcing regulations more strictly, empowering women in the digital sphere, requiring the localisation of vital data, and learning from global best practices.

Conclusion

This article emphasizes the various threats to women's digital rights in India, such as identity theft, cyber stalking, the non-consensual sharing of private or intimate content or information, and financial exploitation. Structural obstacles including low digital literacy, lax enforcement of legal protections, and insufficient institutional procedures exacerbate these dangers. The analysis also demonstrates that although India's legislative framework, particularly the Digital Personal Data Protection Act of 2023 and the Information Technology Act of 2000, offers a regulatory basis, it is still insufficient to address the gendered aspects of online harms. These vulnerabilities are aggravated by the dependence on foreign data storage, since jurisdictional complications impede prompt enforcement and inquiry. Thus, by guaranteeing that vital data is kept on Indian soil, data localisation becomes a potentially effective instrument for protecting women's digital rights. This improves accessibility for law enforcement and fortifies regulatory monitoring.⁴¹

The results point to a number of policy-related issues. In order to ensure that women's data is categorized as sensitive and subject to increased safeguards, gender-specific rules must be implemented in tandem with the execution of the Digital Personal Data Protection Act. Second, technology platforms ought to include proactive compliance measures, such as rapid takedown systems for gender-based cybercrimes and transparency reports.⁴² Through advocacy, awareness-raising campaigns, and computer literacy initiatives catered to women from all socioeconomic backgrounds, civil society organizations can support these initiatives. A strong ecosystem that is not only reactive but also preventive in nature can be created by integrating localization criteria with more comprehensive data protection standards.

Longitudinal studies are required for future research in order to assess how well localization reduces gendered effects on the internet. Research should examine if data

localization results in quicker investigation times, higher success rates for prosecutions, and more effective deterrence against cybercrimes directed at women. Comparative studies between different jurisdictions, like China's Cyber security Law and the European Union's General Data Protection Regulation,⁴³ may offer important insights into potential hazards and best practices. Furthermore, interdisciplinary study that combines gender studies, technology, and law would enhance the conversation by providing comprehensive answers to new problems.⁴⁴

Overall, the conclusion restates that protecting women's digital rights necessitates a multifaceted strategy that combines institutional strengthening, legal reform, and technology protections. Thus Data localisation plays a crucial role in safeguarding Indian women's digital rights and protecting them from exploitation. To establish an ecosystem where women's data is not only safeguarded but also utilized to enable their involvement in the digital economy, policymakers, IT firms, and civil society organizations must work together. India's capacity to turn these promises into tangible action will have a big impact on how its digital world future develops.

References :

1. Sumant Sinha, Leveraging Digital Transformation to Empower Women 7 (ASSOCHAM),
2. Anika Choudhary & Renu Patidar, Women in the Digital Age in India, 7 World Res. Pol. Sci. J. 1 (2024).
3. Giuditta de Prato & Jean Paul Simon, Is Data Really the New "Oil" of the 21st Century or Just Another Snake Oil? Looking at Uses and Users (Private/Public),
4. National Crime Records Bureau, Crime in India Report (2022).
5. Data Security Council of India, Global Data Privacy Risks (2025), 2025 Cyber Security Outlook.
6. Vanita, Jurisdictional Challenges in Cyber Crime Prosecution, 7 Indian J.L. & Legal Rsch. 3391(2024).
7. Jennifer L. O'Donoghue et al., Why We Need to Recommit to Gender Equality (Brookings Institution, Mar. 7, 2025).
8. Information Technology Act, No. 21 of 2000, Sec.66 and Sec.66 A
9. Digital Personal Data Protection Act, No. 22 of 2023, Sec.6, Sec.12 and Sec.18.
10. K. Anvar Sadath, Draft Digital Personal Data Protection Rules 2025: The Goal Remains Distant...? (LiveLaw, Feb. 18, 2025, 6:15 PM IST).
11. Medha Garg, India's Data Protection Act: A Shield for Privacy or a Tool for State Surveillance? (TechPolicy, July 25, 2025), <https://www.techpolicy.press/indias-data-protection-act-a-shield-for-privacy-or-a-tool-for-state-surveillance/>. (accessed Aug.11,2025)
12. Shreya Singhal v. Union of India, (2015) 5 SCC 1"
13. Information Technology Act, No. 21 of 2000, Sec. 67, Sec.67A–67B (obscenity and sexually explicit content)
14. "Sabu Mathew George v. Union of India, (2018) 3 SCC 229.
15. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1."

16. The Information Technology Act, No. 21 of 2000, Secs. 79, 87(2)(zg),.
17. Faheema Shirin R.K. v. State of Kerala, 2019 SCC
18. Plaintiff Filed Over Deepfake Image Used for Blackmail, Times of India (Dec. 27, 2024)
19. Tinsukia Techie Held for Creating, Circulating Morphed Pics Using AI, Times of India (Jul. 14, 2025)
20. 5,000 Lewd Texts, 1,000 Calls: UP Patient Arrested for Harassing Woman Doc, Hindustan Times (Aug. 27, 2025) (India).
21. "K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1"
22. Information Technology Act, 2000, No. 21 of 2000
23. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, Gazette of India, G.S.R. 314(E) (Apr. 16, 2013).
24. Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012.Sec. 11–12, Sec.13–15, Sec.19 (India).
25. Digital Personal Data Protection Act, No. 22 of 2023, Secs. 2(i), 2(p), 2(t), 3, 4–6 (India).
26. Unequal Accessibility in the Digital World Replicates and Further Deepens Discriminatory Patterns in India, in Feminism in India (FII), Gender & Inclusion Conference: Exploring the Intersection of Gender, Technology and Socioeconomic Empowerment, Conference Pre-Reads 23 (2025).
27. Morrison Foerster, Get Ready for India's New Data Privacy Law (Sept. 11, 2023).
28. The Digital Personal Data Protection Act, No. 22 of 2023, Sec 16.
29. Smriti Parsheera & Prateek Jha, Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options? (Carnegie India Working Paper).
30. One Trust / Data Guidance, India: Draft Digital Personal Data Protection Rules, 2025 — Cross-Border Transfers (May 15, 2025).
31. Reserve Bank of India, Storage of Payment System Data: FAQs (June 26, 2019), FAQ No. 2995 (regarding Circular DPSS.CO.OD.No.2785/06.08.005/2017-18, Apr. 6, 2018).
32. Pranesh Prakash, Internet Blocking and Shutdowns in India and International Human Rights Law, 5 Indian Public Pol'y Rev. 38 (2024).
33. UNICEF, Bridging the Gender Digital Divide: Challenges and an Urgent Call for Action for Equitable Digital Skills Development (May2023).
34. Tanusha Tyagi, The Adequacy Dilemma: India's DPDPA and the GDPR (Observer Research Foundation, Expert Speak, Jan. 2025).
35. Harish Yadav, Unveiling the Dark Side of Cyberspace: A Study of Cyber Crimes Against Women in India, IJFANS Int'l Journal of Food & Nutritional Scis., Vol. 11, Iss. 10, 2022, at 3408.
36. GSMA, The Mobile Gender Gap Report 2022.
37. Nat'l Crime Recs. Bureau (NCRB), Crime in India 2022: Statistics (2023).
38. Mark West, Rebecca Kraut & Han Ei Chew, I'd Blush if I Could: Closing Gender Divides in Digital Skills Through Education (UNESCO2019),
39. Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 45,

- 2016 O.J. (L 119) 10
40. Privacy Act 1988 (Cth) Sec.6 (Austl.).
 41. Sai Ramani Garimella & B. Parthiban, Ringfencing Data? — Perspectives on Sovereignty and Localisation from India, in *Blurry Boundaries of Public and Private International Law* 261, 281 (Poomintr Sooksripaisarnkit & Dharmita Prasad eds., 1st ed. 2022).
 42. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, G.S.R. 139(E) (Feb. 25, 2021) (India).
 43. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016 O.J. (L 119) 1.
 44. Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Nov.7, 2016, effective June 1, 2017) (China).