International Journal of Social Science Research and Review

ijssrr.com
editor@ijssrr.com
Volume 9, Issue 11
November 2026
pp. 65–78

Bridging the Gap: Data Privacy and Safety of Women

Nikshit Sharma
The Shri Ram School Aravali, Haryana, India
Corresponding author: sharmanikshit07@gmail.com
DOI: https://doi.org/10.47814/fy6bvs82

Abstract

This paper looks at how far India's Digital Personal Data Protection Act, 2023 actually succeeds in regulating the way companies collect, store, and use personal data, with particular attention paid to the gap left by newer technologies such as deepfakes and AI-generated content. Using doctrinal analysis and comparative reference to the United Kingdom and the European Union, it traces the development of Indian data protection law from the Information Technology Act, 2000 through Justice K.S. Puttaswamy v. Union of India to the 2023 Act. This legal analysis is combined with primary survey data collected from seventy-seven respondents on their awareness, trust, and concern about corporate data handling. The findings show that public concern about how companies use personal data consistently outstrips trust that companies handle it responsibly, and that most respondents were unaware of the DPDP Act itself. The paper argues that while India's framework broadly matches global standards, it is not yet equipped to deal with AI-driven and gender-based harms, and that how effective it turns out to be will depend on enforcement through the Data Protection Board rather than on the text of the law alone.

Keywords: *Data Privacy; Digital Personal Data Protection Act; 2023; Corporate Data Handling; Corporate Accountability; Artificial Intelligence; Deepfakes*

1. INTRODUCTION

Digital technology has grown fast, and it has changed how companies collect, store, process, and use personal information. Personal data is now one of the most valuable things a corporation can have. Companies use it to improve their services, target advertisements, train AI systems, and run their business more efficiently. Social media platforms, e-commerce businesses, banks, healthcare apps, and technology firms all depend heavily on collecting data as part of how they operate. This growing reliance on data has raised real concerns about privacy, surveillance, misuse of personal information, and whether corporations can be held accountable.

Newer technologies, facial recognition, algorithmic profiling, predictive analytics, and generative AI among them, can process huge amounts of personal information quickly and efficiently. These technologies drive innovation and economic growth, but they also raise the risk of data breaches, identity theft, cyber exploitation, and personal information being shared without permission. Data privacy touches on human dignity, individual autonomy, and legal protection in the digital age. It goes well beyond questions of technology or cybersecurity alone.

Today's companies hold huge amounts of user information: financial details, biometric data, communication records, browsing history, and behavioural data, among other things. This makes data protection a central part of corporate governance. Without effective legal regulation, companies collecting too much data combined with weak security systems leaves room for exploitation, manipulation, and misuse.

Several international incidents show what happens when corporate regulation falls short. The Cambridge Analytica scandal, for example, showed how personal data pulled from social media could be used for political profiling and behavioural manipulation without proper consent.[1] Major breaches at Equifax, Meta, and Marriott

[1] Facebook–Cambridge Analytica Data Scandal, Wikipedia (detailing the unauthorised harvesting of data from approximately 87 million Facebook users).

International similarly left millions of users exposed to financial fraud, identity theft, and privacy violations.[2] Incidents like these pushed the demand for stronger legal safeguards and greater corporate accountability worldwide.

India has digitalised quickly over the last decade. Online banking, digital payments, e-commerce, and social media have all driven large-scale corporate collection of personal data. At first India had no comprehensive privacy framework at all. The Information Technology Act, 2000 dealt mainly with cybersecurity and electronic transactions. Privacy was recognised as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a turning point in Indian constitutional law,[3] and this paved the way for the Digital Personal Data Protection Act, 2023, India's first comprehensive data protection statute. The Act requires corporations, called "Data Fiduciaries," to process personal data lawfully, transparently, and securely, and it introduces the principles of consent-based processing, purpose limitation, and data minimisation.[4]

At the same time, deepfakes, algorithmic surveillance, and generative AI capable of producing synthetic media at scale have created new kinds of digital harm. Women bear a disproportionate share of this harm. They are targeted through the non-consensual circulation of AI-generated and manipulated digital content, which exposes just how limited the existing legal framework really is.

This paper sets out to examine India's evolving data protection framework and how well it regulates corporate handling of personal data in the age of AI. The focus is on corporate accountability and whether existing law is adequate, using the United Kingdom and the European Union as points of comparison against global standards. Through doctrinal and comparative analysis, it asks whether current legal frameworks can balance innovation, corporate interests, and individual privacy in an increasingly digital world.

2. LITERATURE REVIEW

2.1 Historical Evolution

Data collection used to be a manual exercise, limited to paper-based records. That changed in the latter half of the twentieth century, when computers made it possible to store and process information at a scale that had never existed before. The shift accelerated further with the internet, mobile technology, and cloud computing, which made data collection continuous and largely invisible to the people it concerned. For much of this period, data was treated mainly as a commercial and administrative resource. Corporations' growing use of personal information for profit eventually drew global attention to questions of privacy and surveillance.

Technology companies such as Google, Microsoft, and Amazon, social media platforms including Facebook, Instagram, and X, and financial institutions such as PayPal and JPMorgan Chase began collecting large volumes of user data for targeted advertising, behavioural analysis, and algorithmic profiling, often faster than legal systems could keep up. One of the earliest international responses was the OECD's 1980 Privacy Guidelines. These set out principles of purpose limitation, data security, accountability, and consent. They were not binding, but they still shaped legislation around the world.[5] The European Union became the strongest advocate of comprehensive regulation, a push that led to the General Data Protection Regulation of 2018, while the United Kingdom developed a parallel post-Brexit framework.[6] High-profile incidents such as the Cambridge Analytica scandal[7] and the Equifax and Marriott breaches[8] further showed what weak regulation could lead to.

India's data protection law took shape slowly, over several stages. The Information Technology Act, 2000 was centred on cybersecurity, though Section 43A did impose liability on body corporates for negligent security practices.[9] The IT (Reasonable Security Practices) Rules, 2011 went a step further and recognised categories such

[2] Equifax Inc., Equifax Announces Cybersecurity Incident Involving Consumer Information, U.S. SEC, Form 8-K (Sept. 7, 2017).

[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[4] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

[5] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).

[6] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1; Data Protection Act 2018, c. 12 (U.K.).

[7] Facebook–Cambridge Analytica Data Scandal, Wikipedia (detailing the unauthorised harvesting of data from approximately 87 million Facebook users).

[8] Equifax Inc., Equifax Announces Cybersecurity Incident Involving Consumer Information, U.S. SEC, Form 8-K (Sept. 7, 2017).

[9] The Information Technology Act, 2000, § 43A, No. 21 of 2000, as inserted by the IT (Amendment) Act, 2008.

as financial and biometric data as "sensitive personal data," though enforcement remained weak.[10] Constitutional privacy law developed through *Kharak Singh v. State of Uttar Pradesh*, which linked unauthorised intrusion to personal liberty under Article 21,[11] and *R. Rajagopal v. State of Tamil Nadu*, which recognised a right to stop the publication of personal information without consent.[12] This line of cases reached its high point in *Puttaswamy*, where a nine-judge Bench unanimously held that privacy is a fundamental right, including its informational and digital dimensions.[13]

After *Puttaswamy*, the Justice B.N. Srikrishna Committee examined excessive corporate data collection, weak consent mechanisms, and the need for a comprehensive legal framework.[14] Its recommendations later informed the Digital Personal Data Protection Act, 2023.[15] More recently, facial recognition, generative AI, and deepfakes have created harms that existing frameworks were never built to handle, with women disproportionately targeted through the non-consensual circulation of images, as Chapter 4 examines.

This history shows a gradual shift, away from narrow cybersecurity regulation and toward recognising privacy as a constitutional issue, a human rights issue, and a corporate governance issue all at once. Alongside that shift sits a growing need for legal frameworks that can actually keep up with fast-moving technological threats.

2.2 Data Protection in the Corporate World

Corporate data practices are shaped by commercial incentives, technological capacity, and legal obligation. This chapter looks at the obligations placed on companies under Indian and comparative law, how those obligations are enforced, and where the framework falls short.

Privacy and Security. Data privacy is about individuals' control over their own personal information. Data security is about the technical and organisational measures that stop unauthorised access or loss. In practice, a security failure almost always turns into a privacy violation. Once a corporation suffers a breach, sensitive financial, biometric, or medical information gets exposed without consent, which is exactly why strong security measures matter so much for real privacy protection. Because personal data carries real commercial value, profit-driven incentives often push companies toward collecting as much as possible, holding onto it longer than needed, and monetising it through third parties, while ransomware and phishing threats add further risk for users whose data is not properly protected.

Global Frameworks. Binding obligations around the world range from the EU's extraterritorial GDPR[16] to the UK's post-Brexit Data Protection Act, administered by the Information Commissioner's Office,[17] to the fragmented, sector-specific model followed in the United States.[18] Before 2023, India relied on the IT Act, 2000 and the 2011 Rules, which gave only a limited basis for corporate liability. This was a gap the DPDP Act was designed to close, and one discussed comparatively in Chapter 5.

DPDP Act Obligations. The DPDP Act, 2023 classifies corporations as "Data Fiduciaries" and is built around a consent-based model. Personal data can be processed only once free, specific, informed, and unambiguous consent has been given, along with clear notice of why it is being collected.[19] Purpose limitation guards against "function creep," and data minimisation keeps collection to what is strictly necessary.[20] Fiduciaries must put "reasonable security safeguards" in place, and if a breach happens, they must notify the Data Protection Board of India and the individuals affected. This formal mechanism did not exist under the prior regime, and the Board can

[10] The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

[11] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

[12] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[14] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (MeitY, 2018).

[15] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

[16] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1; Data Protection Act 2018, c. 12 (U.K.).

[17] Data Protection Act 2018, c. 12 (U.K.); Information Commissioner's Office, About the ICO, ico.org.uk.

[18] HIPAA, Pub. L. No. 104-191; COPPA, 15 U.S.C. §§ 6501–6506; Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809; California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq.; California Privacy Rights Act of 2020.

[19] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

[20] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

now impose penalties running into hundreds of crores of rupees.[21] Data Principals, in turn, are granted rights of access, correction, erasure, and nomination, which means corporations have to build accessible ways for people to actually exercise those rights.[22]

Cross-Border Application. The Act extends to foreign Data Fiduciaries that process Indian personal data, closing a gap that previously let foreign platforms sidestep Indian privacy norms. Cross-border transfers are permitted to countries notified as meeting adequate protection standards, an approach similar to GDPR adequacy decisions, though the implementing rules are still pending. This is different from the stricter data-localisation requirements the RBI has long imposed on banking data.[23]

Sectoral Overlap. Corporations also answer to the RBI on data localisation, SEBI on market-intermediary data governance, IRDAI on policyholder data, and CERT-In's 2022 cybersecurity reporting guidelines.[24] How the Data Protection Board is supposed to coordinate with these sectoral regulators is still unclear.

Enforcement Gaps. How much the Act achieves in practice depends on the Data Protection Board actually being set up, and on subordinate rules that are still pending. Until these are operational, enforcement will stay limited. Many corporations, smaller enterprises especially, lack the technical and financial capacity for full compliance. Consent mechanisms often prioritise user engagement over consent that is genuinely informed, burying it inside complex privacy policies instead. This accountability gap is widened further by the imbalance of knowledge and power between corporations and individual users, particularly those in non-urban areas or with limited digital literacy. Meaningful accountability needs strong legislation paired with accessible enforcement, active oversight, and public awareness. The DPDP Act is a significant step forward, but how effective it actually proves will depend on implementation, and on corporations doing more than the bare minimum.

2.3 Gender And Data Privacy Concerns

Data privacy has a gendered side that most legal frameworks fail to account for. The law treats individuals as one undifferentiated category of data subjects, but in practice women and gender minorities face surveillance, harassment, and exploitation that is both more frequent and more severe than what the general population experiences.

The Gendered Nature of Digital Harm. The clearest example of this is the non-consensual circulation of intimate images, which overwhelmingly targets women. National Crime Records Bureau figures show reported cases of publishing or transmitting sexually explicit material without consent climbing from 1,896 in 2021 to 2,251 in 2022, a trend tied to wider smartphone and messaging access.[25] The harm goes well beyond reputational damage. It extends to psychological trauma, forced withdrawal from public life, and, in documented cases, self-harm and suicide.

Deepfake technology adds another layer of risk. Unlike conventional image-based abuse, it needs no original intimate image at all. Content is fabricated instead by superimposing a real person's face onto synthetic media. Studies conducted in the UK and US have found that over ninety percent of deepfake content online is non-consensual pornography, overwhelmingly targeting women,[26] and India has seen a fast rise in such cases, including several involving public figures, which shows just how little in the way of specific legal remedies actually exists.

Women are also disproportionately exposed to stalkerware, software installed covertly to track location, communications, and behaviour. Kaspersky Lab research has repeatedly placed India among the three countries worldwide most affected by stalkerware,[27] a form of surveillance that often shows up in domestic or intimate-partner settings and one that Indian law has been slow to address.

Existing Legal Frameworks and Their Limitations. India's legal response has been piecemeal and reactive. Provisions in the Indian Penal Code on obscenity and harassment predate the digital era. Section 354A criminalises sexual harassment and Section 509 addresses conduct that outrages a woman's modesty, but both require proof of

[21] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).
[22] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).
[23] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).
[24] RBI, Master Directions on Digital Payment Security Controls (2021); SEBI, Cyber Security and Cyber Resilience Framework; IRDAI, Guidelines on Information and Cyber Security for Insurers (2017); CERT-In Directions under § 70B(6) of the IT Act, 2000 (2022).
[25] National Crime Records Bureau, Crime in India 2022: Statistics, ncrb.gov.in.
[26] Henry Ajder et al., The State of Deepfakes: Landscape, Threats, and Impact, Deeptrace (2019); Moncarol Y. Wang, Don't Believe Your Eyes: Fighting Deepfaked Nonconsensual Pornography with Tort Law, 2022 U. Chi. L. Forum 415.
[27] Kaspersky, The State of Stalkerware 2023, Securelist (2024); The State of Stalkerware 2022, Securelist (2023).

intent and say nothing about the structural dynamics of online abuse.[28] Section 66E of the IT Act criminalises capturing or transmitting intimate images without consent, and Section 67A penalises publishing sexually explicit material electronically.[29] These are meaningful provisions, but they are narrow. They do not extend to deepfakes, they create no civil remedy, and enforcement is inconsistent at best. The IT (Intermediary Guidelines) Rules, 2021 require platforms to acknowledge privacy complaints within twenty-four hours and resolve them within fifteen days,[30] though enforcement here too has been uneven, with delayed responses and content that has already been removed simply getting re-uploaded. The DPDP Act is consent-based and aimed at lawful corporate processing, so it does not reach gendered digital harm or the misuse of synthetic media by individual bad actors.

Comparative Approaches. Other jurisdictions tackle these gaps more directly. The UK's Online Safety Act, 2023 criminalises sharing or threatening to share intimate images, deepfakes included, and places platforms under a duty to proactively prevent such content.[31] A later statute, the Data (Use and Access) Act, 2025, separately criminalised the *creation* of non-consensual sexually explicit deepfakes, closing a gap the 2023 Act had left open.[32] Australia's Online Safety Act, 2021 takes a different route, combining civil penalties for non-consensual image sharing with an eSafety Commissioner empowered to issue removal notices within twenty-four hours.[33] India has no equivalent legislation. Parliamentary committees have acknowledged the need for a dedicated law, but none has followed yet.[34]

Toward a Gender-Responsive Framework. Indian data privacy law treats gender as incidental rather than structural. The DPDP Act does not ask Fiduciaries to assess gender-specific risks, does not impose heightened obligations where data is disproportionately weaponised against women, and creates no dedicated remedy for the harms women most commonly encounter online. A genuinely gender-responsive framework would need civil and criminal liability for people who create and distribute non-consensual intimate images, synthetic ones included, along with mandatory and swift platform removal obligations backed by enforceable penalties, dedicated support mechanisms for survivors, and formal recognition that certain categories of processing carry an elevated gender-specific risk.

2.4 Comparative Study: India In A Global Context

The European Union. In force since May 2018, the GDPR remains the global benchmark. It applies extraterritorially to any organisation that processes EU residents' data regardless of where it is located, which means Indian companies serving European customers are bound by it too.[35] It shares core features with the DPDP Act, among them consent-based processing and rights of access and erasure, but it goes further still. It requires mandatory data protection impact assessments and data protection officers for large-scale processors, and it sets penalties of up to four percent of global turnover or twenty million euros, a regime that has produced major fines against Meta, Amazon, and Google.[36] The DPDP Act's penalty structure, while significant, is not tied to turnover, which may blunt its deterrent effect on multinationals. The GDPR also gives greater protection to special categories of sensitive data, health, biometric, sexual orientation, and political opinion among them, a distinct category the DPDP Act still leaves to unfinished subordinate rules. This gap bears directly on the gendered harms discussed above.

The United Kingdom. After Brexit, the UK kept GDPR standards in place through the Data Protection Act, 2018 and UK GDPR, enforced by an active Information Commissioner's Office.[37] This framework matters to India for two reasons. Adequacy determinations will shape how easily Indian companies can access British markets, and UK legislation such as the Online Safety Act, 2023 shows that data protection law and online safety law can be developed side by side, a model India has not followed yet.

---

[28] The Indian Penal Code, 1860, §§ 354A, 509, No. 45 of 1860.

[29] The Information Technology Act, 2000, §§ 66E, 67A, as inserted by the IT (Amendment) Act, 2008.

[30] The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r. 3(2) (India).

[31] Online Safety Act 2023, c. 50, § 188 (U.K.) (amending the Sexual Offences Act 2003, c. 42, § 66B).

[32] Data (Use and Access) Act 2025, c. 13, § 138 (U.K.) (inserting § 66D into the Sexual Offences Act 2003).

[33] Online Safety Act 2021 (Cth) pt 6 (Austl.); eSafety Commissioner, Image-Based Abuse, esafety.gov.au.

[34] Parliamentary Committee on Empowerment of Women, Cyber Crimes and Cyber Safety of Women, Fourth Report (2026) (Parliament of India).

[35] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1; Data Protection Act 2018, c. 12 (U.K.).

[36] Irish Data Protection Commission, Decision re Meta Platforms Ireland Ltd. (May 2023) (€1.2 billion fine); Luxembourg CNPD, Decision re Amazon Europe Core S.à r.l. (July 2021) (€746 million fine); CNIL, Decision re Google LLC (Jan. 2022).

[37] Data Protection Act 2018, c. 12 (U.K.); Information Commissioner's Office, About the ICO, ico.org.uk.

The United States. The US has no comprehensive federal privacy law. It relies instead on sector-specific statutes such as HIPAA, COPPA, and Gramm-Leach-Bliley, backed up by state laws including the California Consumer Privacy Act and California Privacy Rights Act, and enforcement is uneven across the FTC and state regulators.[38] This fragmented model shows that the absence of unified regulation does not just mean weaker protection. It also breeds confusion, regulatory arbitrage, and outcomes that vary a great deal from state to state.

India in Comparative Perspective. The DPDP Act sits in a middle position. It is far more comprehensive than the previous IT Act framework and broadly in step with the global mainstream on consent, purpose limitation, and breach notification, with a meaningful extraterritorial reach of its own. Gaps remain nonetheless. There is no primary-legislation category for sensitive data, no mandatory data protection officer requirement, and no turnover-based penalty regime, and the Act's central institution, the Data Protection Board of India, has yet to be made operational, which leaves much of this comparative picture provisional. Effective data protection, in the end, needs strong legislation matched by a functioning enforcement ecosystem: resourced regulators, accessible complaint mechanisms, a genuine corporate compliance culture, and public awareness. India has made real legislative progress, but the distance between law on the books and law in practice remains substantial. The experiences of the EU, UK, and, more cautiously, the US offer useful lessons for closing that distance.

3. PRIMARY RESEARCH

The doctrinal analysis in the earlier chapters sets out what the law says about how companies in India are meant to handle personal data. This chapter asks how far that law tracks public experience and expectation on the ground. A structured questionnaire was used to gauge awareness of corporate data practices, trust in how companies handle that data, and perceptions of the risks posed by artificial intelligence and deepfake technology. This adds an empirical account of public perception to the doctrinal analysis above.

3.1 Methodology

The survey used a non-probability convenience sampling method, distributed through personal and professional networks, and produced seventy-seven usable responses. Most respondents were working professionals (59.7%), followed by business owners (22.1%) and students (14.3%), with the remainder in other occupations (3.9%). Because most respondents are active in the workforce or in business, their answers carry particular weight for a study of how companies handle personal data. The questionnaire had nineteen closed questions spanning five broad areas: general digital habits, awareness of corporate data collection and the DPDP Act, concern and trust and perceived corporate transparency, familiarity with AI-generated content and deepfakes and how these affect online behaviour, and views on legal responsibility and reform.

3.2 Data Analysis

Responses were analysed descriptively through frequency distributions and percentages, and selected variables were cross-tabulated to check whether awareness of a risk correlated with attitudinal or behavioural change. Given the convenience sample and its modest size, no claim is made that the results are statistically representative of the Indian population as a whole. The survey is instead treated as an indicative account of perception among a mixed cross-section of digital users, to be read alongside the doctrinal material in Chapters 2 through 5.

4. RESULTS

4.1 Digital Habits

Nearly half of all respondents use digital platforms every day (49.4% daily, 23.4% weekly, 20.8% occasionally, 6.5% rarely). This means most participants are in regular contact with companies that collect personal information, which makes data privacy an issue that touches their daily lives directly.

4.2 Awareness of Data Collection and Statutory Protection

Although a slight majority understand that companies collect personal information (54.5% aware, 45.5% not), almost half remain unaware. This shows that public awareness of corporate data practices stays limited despite widespread internet use (Figure 1). Awareness of the specific statute meant to govern that collection was lower still. Most respondents had not heard of India's Digital Personal Data Protection Act, 2023, with only 40.3% aware of it against 59.7% who were not. This points to a substantial awareness gap, even though the Act is India's primary data protection legislation.

[38] HIPAA, Pub. L. No. 104-191; COPPA, 15 U.S.C. §§ 6501–6506; Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809; California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq.; California Privacy Rights Act of 2020.

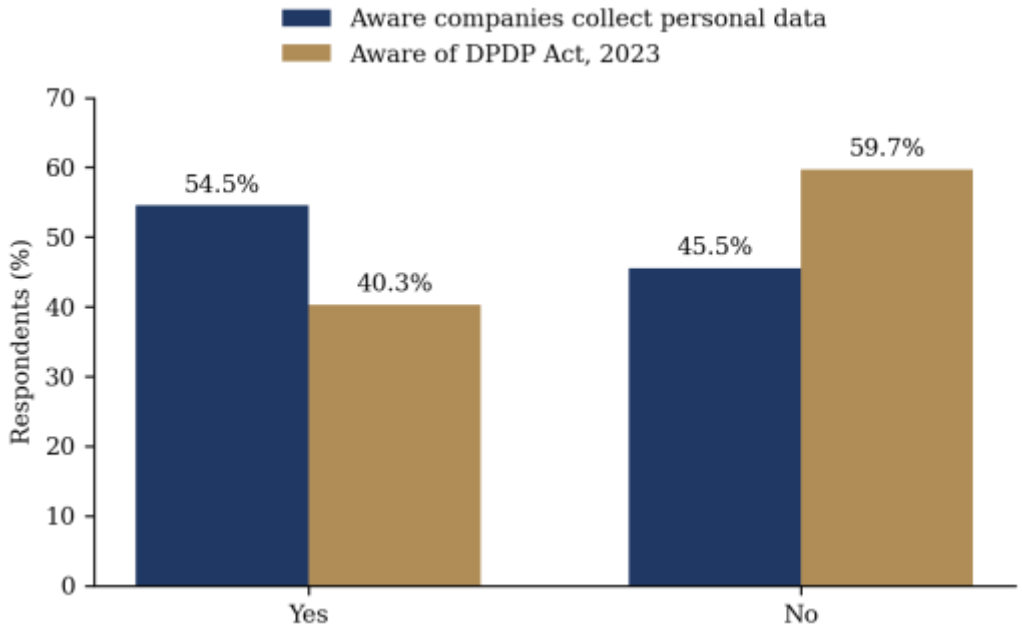


Figure 1. Awareness of corporate data collection and of the DPDP Act, 2023 (n = 77).

4.3 Concern, Reading Habits, and Trust

On a five-point scale, most respondents' concern about corporate handling of their data fell between moderate and high (32.5% at the midpoint, 41.6% rating four or five). This suggests that while people recognise data privacy as an important issue, many may not fully grasp the risks involved. Despite this concern, only around one in five respondents (22.1%) said they always read privacy policies, with 39.0% doing so only sometimes, 27.3% rarely, and 11.7% never. This suggests that informed consent exists more in theory than in practice. Trust in companies to protect personal information was correspondingly weak: 48.1% reported low trust against only 23.4% reporting high trust (Figure 2). This weak trust supports the case for stronger accountability mechanisms and better corporate governance.

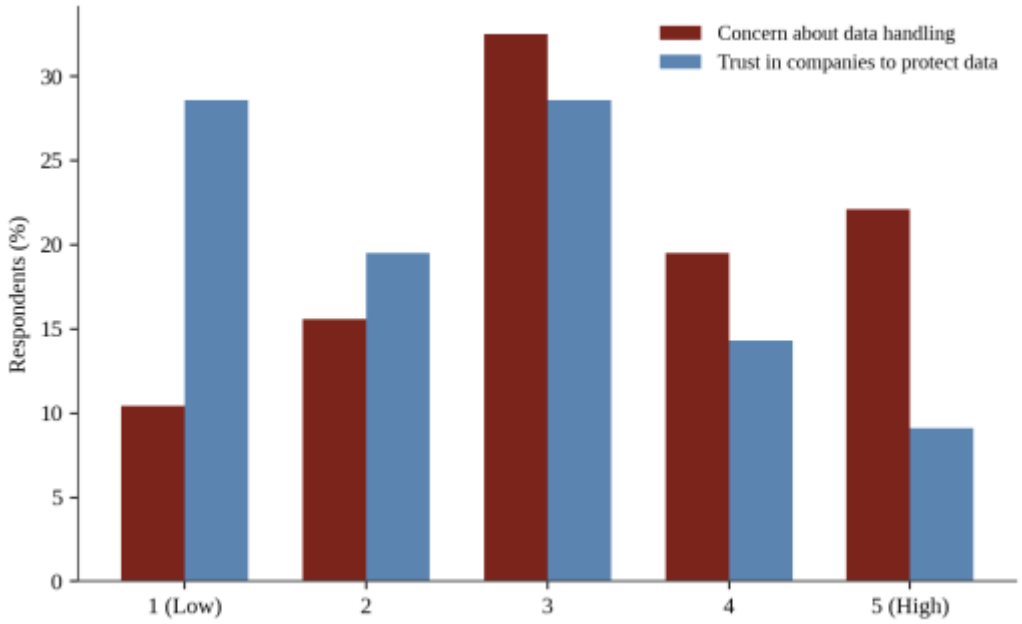


Figure 2. Self-reported concern about data handling compared with trust in companies, on a five-point scale (n = 77).

4.4 Perceived Transparency and Corporate Conduct

A clear majority, 57.1%, believe companies are not transparent about how they use personal information, against 15.6% who believe they are and 27.3% who are unsure (Figure 3). This reflects low public confidence in

corporate disclosure practices. More than half of respondents have experienced personalised advertising (35.1% frequently, 23.4% occasionally), which points to how widespread behavioural data collection has become. A significant share, 39.0%, also believe companies collect more information than necessary, and the large "unsure" category of 32.5% suggests uncertainty about what data corporations are actually allowed to collect. Nearly half of respondents, 46.8%, support stricter legal penalties for corporate data breaches, which points to growing expectations of stronger regulatory enforcement.

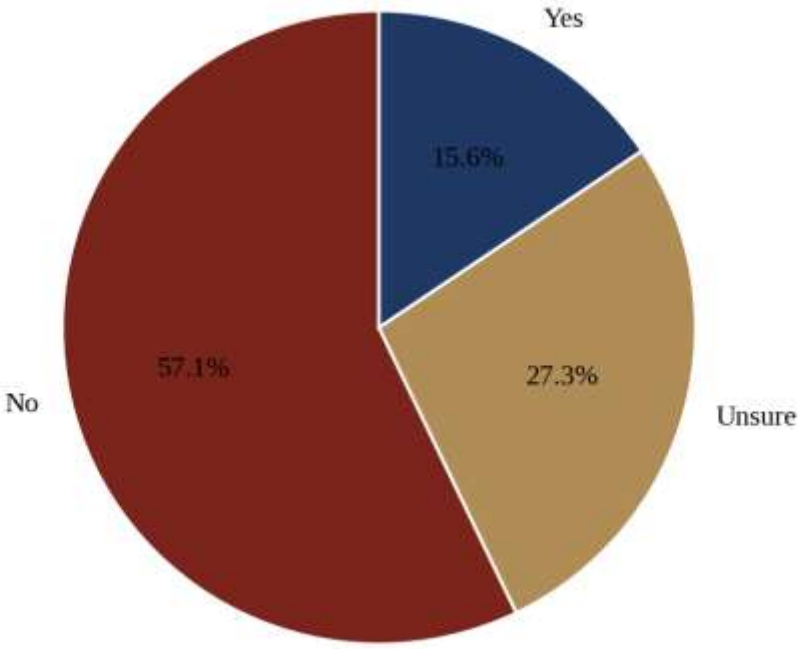


Figure 3. Perceived transparency of companies regarding personal data use (n = 77).

4.5 AI, Deepfakes, and Risk Perception

Despite how much AI gets discussed, more than half of respondents (57.1%) are unfamiliar with deepfake technology, against 42.9% who are familiar with it. This suggests that awareness efforts have not kept pace with the technology itself. Only a small minority, 13.0%, believe existing laws adequately regulate AI-related privacy risks, while 41.6% believe they do not, and a large share, 45.5%, are unsure about India's legal framework here. Around two in five respondents (37.7%) report becoming more cautious about sharing personal information online because of concerns about AI and deepfakes, while a further 37.7% are unsure whether their behaviour has changed at all.

Looking more closely at this last figure, familiarity with deepfakes tracked closely with reported caution. Among respondents unfamiliar with the technology, only 20.5% reported becoming more cautious, and over half were unsure whether their behaviour had changed at all. Among those familiar with the technology, that figure rose to 60.6% (Figure 4). This pattern suggests that caution comes from understanding a risk, not from the risk itself, which stays roughly the same for everyone whether or not they recognise it.

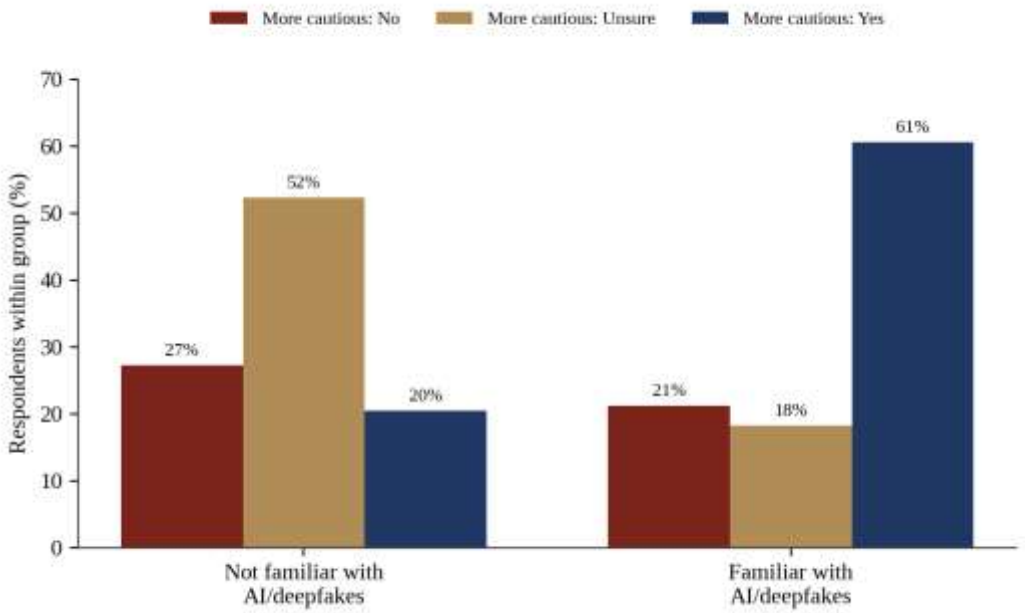


Figure 4. Reported increase in online caution attributable to AI and deepfake concerns, by prior familiarity with the technology (n = 77).

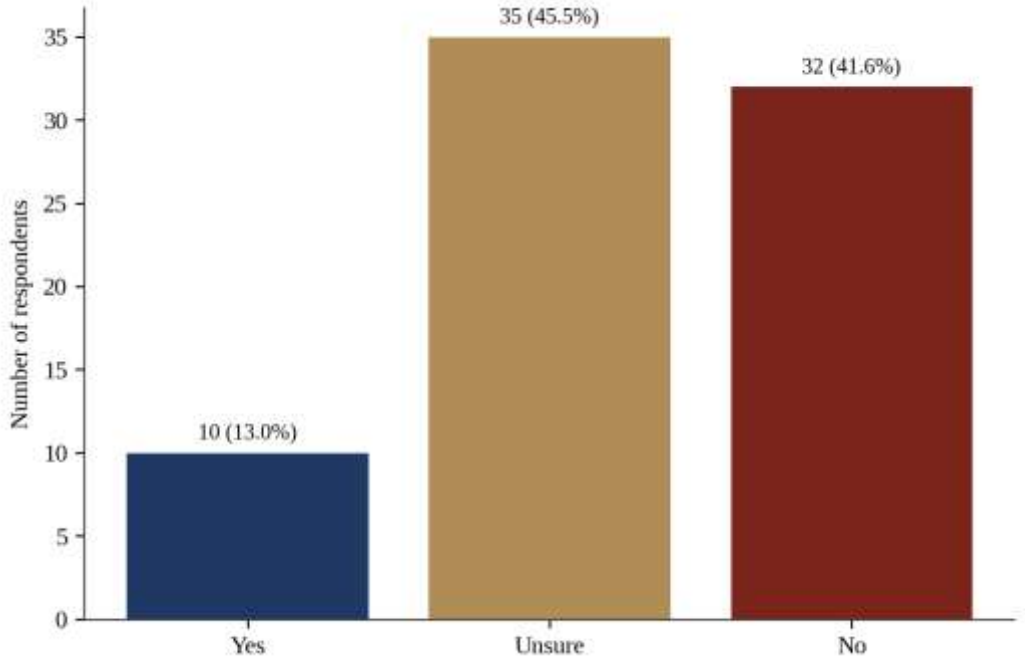


Figure 5. Perceived sufficiency of existing law to regulate AI-related privacy risks (n = 77).

4.6 Primary Concerns

Asked which risk concerned them most, respondents were fairly evenly split. Sale of personal data (24.7%) and identity theft (24.7%) topped the list, followed by deepfakes (20.8%), online surveillance (16.9%), and data breaches (13.0%) (Figure 6). Respondents seem most concerned about the commercial exploitation of personal information and identity theft, more than traditional cybersecurity incidents, which fits this paper's focus on corporate data governance.

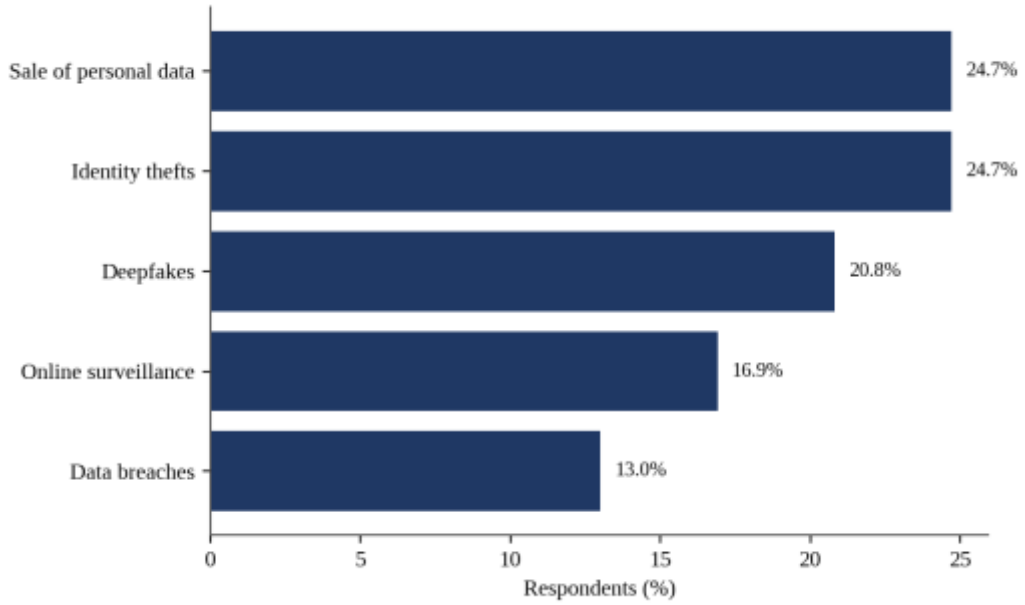


Figure 6. Primary privacy concern reported by respondents (n = 77).

4.7 Legal Awareness, Reform, and Responsibility

Support for stronger data protection laws exceeds opposition (40.3% in favour against 20.8% opposed), though many respondents, 39.0%, remain uncertain, pointing to limited public understanding of the current legal framework. Asked who should bear the greatest responsibility for protecting personal data, the largest group, 28.6%, named corporations, followed by shared responsibility (27.3%), government (23.4%), and individual users (20.8%) (Figure 7). This finding speaks directly to this paper's central focus on corporate accountability, though the near-even spread across all four options suggests the public does not see this as a settled question.

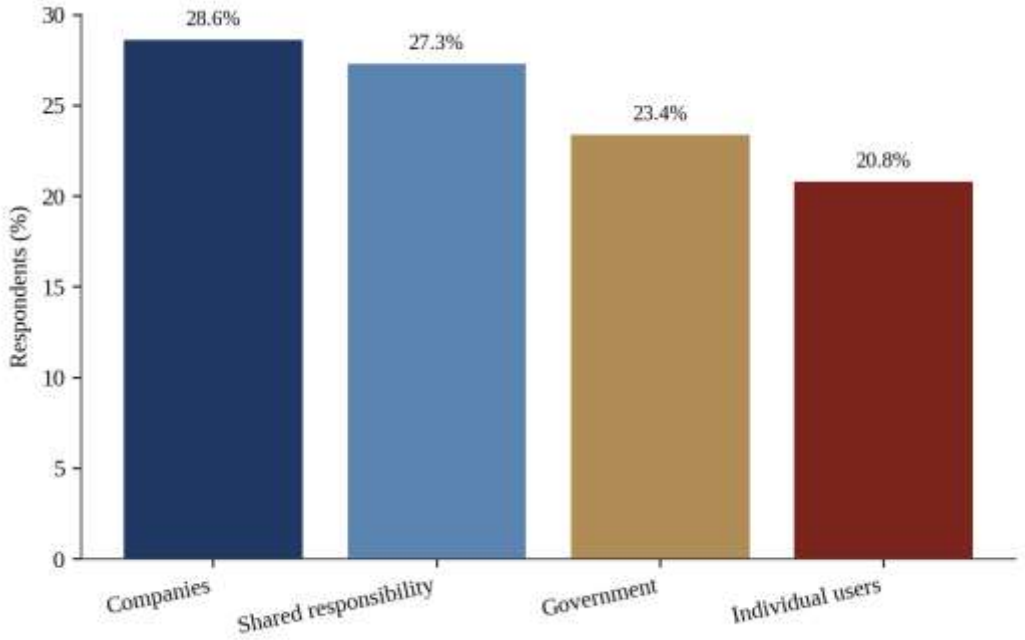


Figure 7. Attribution of primary responsibility for protecting personal data (n = 77).

5. DISCUSSION

Read together with the legal analysis in Chapters 2 to 5, the survey results point to a particular kind of gap. People are not indifferent to their data. Their concern simply is not matched by a clear understanding of what legal protection actually exists. Respondents were more worried about how their data is handled than confident that companies would protect it well, and fewer than half had even heard of the DPDP Act. The writer Shoshana Zuboff

has argued that large technology companies benefit from keeping their data practices unclear, since users who do not fully grasp how their data is used are less likely to push back against it.[39] This idea holds up reasonably well in India too. The finding that 57.1% of respondents doubted companies are transparent about how they use personal data fits Zuboff's argument. It is worth noting, though, that her work is based mainly on companies in the United States and Europe, and Indian companies, many of them smaller or still developing their data practices, may not all operate in quite the same way.

The data also reflect what researchers call the privacy paradox: people report being concerned about their data yet keep using the same platforms and sharing the same information regardless.[40] Almost half the respondents in this survey used digital platforms daily, even though their concern about data handling was higher than their trust in the companies running those platforms. This does not necessarily mean people do not care. It more likely means avoiding these platforms is simply not practical in everyday life, particularly for banking, shopping, or staying in touch with others.[41] This matters for how the DPDP Act works in practice, since the Act assumes a person's consent is meaningful only where they are genuinely free to refuse it, and the privacy paradox suggests that in reality, many users do not feel they have that choice.

A clear link also emerged between how familiar respondents were with deepfakes and how cautious they were about sharing personal information online. Those who understood the technology were roughly three times more likely to report having become more careful. This fits a fairly intuitive idea from psychology, that people take a risk seriously only once they understand it well enough to feel threatened by it.[42] It also carries a worrying implication for the gender-related harms discussed in Chapter 4. If caution depends on understanding the risk, and over half the respondents in this survey did not understand deepfake technology at all, then many of the people most likely to be targeted by it, women in particular, may be the least prepared to protect themselves. The legal scholar Danielle Citron has argued that harms such as non-consensual deepfakes need their own specific legal protection instead of being folded into ordinary data privacy law, precisely because consent-based rules do not capture this kind of harm well.[43] This argument fits India's situation closely, since, as Chapter 4 showed, Indian law currently has no dedicated legal response to deepfakes at all.

Daniel Solove, another legal scholar, has pointed out that privacy problems are not all of a kind. Some involve companies collecting data, some involve how that data is processed, and others involve it being shared or misused entirely without consent.[44] Indian law, through the DPDP Act, deals mainly with the first two, since it is built around consent and limits on how data can be used. The problems raised by AI and deepfakes in this study fall into the category the Act does not really reach, sharing and misuse without consent, which may explain why 41.6% of respondents doubted that existing law was sufficient for AI-related risks specifically, a higher figure than the doubt expressed about data protection law in general. This suggests that simply extending the DPDP Act may not be enough on its own. AI-related harm may need a somewhat different legal approach altogether.

It is also worth noting that awareness of the DPDP Act itself made little difference to whether respondents wanted stronger data protection laws. People who had never heard of the Act wanted stronger protection almost as often as those who had. This suggests that people's views on the law depend less on what they actually know about it than on their everyday experience with companies and technology.[45] If that is right, public awareness campaigns about the DPDP Act may not achieve a great deal on their own. What is more likely to build public trust is people actually seeing the law work, through visible enforcement action, for instance, once the Data Protection Board is properly set up.

Finally, respondents were almost evenly split on who should carry the greatest responsibility for protecting personal data, companies, government, or individuals, which suggests there is no single, obvious answer to this question in the public mind. This is a useful reminder for policymakers. A system that places the entire burden on

[39] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019).

[40] Susan B. Barnes, A Privacy Paradox: Social Networking in the United States, 11 First Monday (2006); Spyros Kokolakis, Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon, 64 Computers & Security 122 (2017).

[41] Susan B. Barnes, A Privacy Paradox: Social Networking in the United States, 11 First Monday (2006); Spyros Kokolakis, Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon, 64 Computers & Security 122 (2017).

[42] Ronald W. Rogers, A Protection Motivation Theory of Fear Appeals and Attitude Change, 91 J. Psychol. 93 (1975).

[43] Danielle Keats Citron, Sexual Privacy, 128 Yale L.J. 1870 (2019).

[44] Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).

[45] Patricia Ewick & Susan S. Silbey, The Common Place of Law: Stories from Everyday Life (1998).

companies, or entirely on individual users being more careful, is unlikely to match what people actually expect. A more balanced approach, where companies are held to enforceable standards while government regulators stay actively involved, would likely fit public expectations better, though this remains difficult in practice for as long as the Data Protection Board stays unconstituted.[46]

6. LIMITATIONS OF THE STUDY

This study has some limitations worth keeping in mind. The seventy-seven respondents were recruited through convenience sampling rather than random selection, so the results are not representative of the Indian population as a whole, and the sample skews toward working professionals with above-average digital exposure. The survey also relies on self-reported behaviour rather than observed behaviour, which may make respondents sound more cautious than they actually are, a limitation the privacy paradox research discussed earlier already points to. Similarly, the link found between familiarity with deepfakes and reported caution shows that the two are connected, not that one directly causes the other. It is possible that people who are generally more risk-averse were simply also more likely to have looked into deepfakes in the first place. Finally, the legal chapters draw on secondary sources and reported court decisions rather than interviews with regulators or company compliance staff, which would have given a fuller picture of how the DPDP Act is actually being implemented while the Data Protection Board remains non-operational.

7. POLICY RECOMMENDATIONS

Several practical reforms follow from reading the legal analysis and the survey data together. First, the Data Protection Board of India should be constituted and made operational without further delay, since its absence leaves the Act without any real enforcement mechanism, and, as the survey shows, without the visible track record that might close the gap between legal awareness and public confidence. Second, companies should be required to give clearer, shorter privacy notices written in plain language, rather than long legal documents that most users never read in full. The finding that most respondents rarely read privacy policies carefully suggests the current format simply is not working. Third, subordinate legislation on sensitive personal data categories, health, biometric, and sexual data among them, should be finalised so the Act extends stronger protection to the categories most exposed to gendered harm, as the European comparison in Chapter 5 shows.

Fourth, large technology companies and social media platforms should be required to publish regular AI transparency reports explaining how their AI systems use personal data and what safeguards exist against the misuse of AI-generated content, since the survey found that most respondents doubted whether existing law was sufficient to deal with AI-related risks. Fifth, independent audits of how companies actually handle personal data, rather than reliance on companies' own compliance claims, would help close the trust gap this study identified, where respondents' concern about data handling ran considerably higher than their trust in companies to manage it responsibly. Sixth, platforms should carry more responsibility for AI-generated harmful content such as deepfakes, including faster and mandatory takedown timelines and dedicated support channels for victims, similar to the models adopted in the United Kingdom and Australia discussed in Chapter 4. Penalties under the Act could also be linked to a company's turnover, as under the GDPR, so fines are large enough to genuinely deter big technology companies instead of being absorbed as a routine cost of doing business.

8. CONCLUSION

This paper set out to examine how far India's evolving data protection framework actually regulates the way companies handle personal data, especially given new challenges such as AI-generated content. The legal analysis shows that India has moved, in under a decade, from having almost no privacy law to a proper, rights-based statute broadly in line with global standards, though one that is still not fully implemented and not yet well equipped to deal with AI-driven and gender-based harms. The survey findings add another layer to this picture. People are more worried about how companies handle their data than they trust companies to handle it well, and, more importantly, most people still know very little about the DPDP Act itself. Respondents who had never heard of the Act wanted stronger protection almost as often as those who had, and people were cautious about deepfakes only once they already understood the technology, even though the underlying risk is roughly the same for everyone.

Looking ahead, the real test for India's data protection framework will not be how well the law reads on paper. It will be whether institutions like the Data Protection Board actually function, whether companies are held to standards they cannot quietly ignore, and whether protection against AI-generated harm keeps pace with the technology itself. As artificial intelligence becomes a bigger part of everyday life, the line between a company

[46] Ian Ayres & John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate (1992).

simply processing data and a company enabling real harm, deepfakes being the clearest example, will only grow harder to draw. How India responds to that shift, through enforcement, corporate responsibility, and public awareness working together rather than any one of them alone, will likely decide whether the DPDP Act becomes a meaningful safeguard or just another well-intentioned law that cannot keep pace with the technology it was written to regulate.

ETHICAL CONSIDERATIONS

Participation in the survey underlying Chapters 3 and 4 was voluntary and anonymous; respondents were informed that their responses would be used for this research paper, and no personally identifying information was collected.

The author declares no conflict of interest.

REFERENCES

Ajder, H., et al. (2019). *The state of deepfakes: Landscape, threats, and impact.* Deeptrace.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate.* Oxford University Press.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*.

California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq.

California Privacy Rights Act of 2020.

CERT-In. (2022). Directions under § 70B(6) of the IT Act, 2000.

Citron, D. K. (2019). Sexual privacy. *Yale Law Journal, 128*, 1870.

CNIL. (2022, January). Decision re Google LLC.

Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians.* MeitY.

COPPA, 15 U.S.C. §§ 6501–6506.

Data (Use and Access) Act 2025, c. 13, § 138 (U.K.) (inserting § 66D into the Sexual Offences Act 2003).

Data Protection Act 2018, c. 12 (U.K.).

The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

Equifax Inc. (2017, September 7). *Equifax announces cybersecurity incident involving consumer information* (Form 8-K). U.S. Securities and Exchange Commission.

eSafety Commissioner. (n.d.). *Image-based abuse.* https://esafety.gov.au

Ewick, P., & Silbey, S. S. (1998). *The common place of law: Stories from everyday life.* University of Chicago Press.

Facebook–Cambridge Analytica data scandal. (n.d.). In *Wikipedia.* (detailing the unauthorised harvesting of data from approximately 87 million Facebook users)

Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809.

HIPAA, Pub. L. No. 104-191.

The Indian Penal Code, 1860, §§ 354A, 509, No. 45 of 1860.

Information Commissioner's Office. (n.d.). *About the ICO.* https://ico.org.uk

The Information Technology Act, 2000, § 43A, No. 21 of 2000, as inserted by the IT (Amendment) Act, 2008.

The Information Technology Act, 2000, §§ 66E, 67A, as inserted by the IT (Amendment) Act, 2008.

IRDAI. (2017). *Guidelines on information and cyber security for insurers.*

Irish Data Protection Commission. (2023, May). Decision re Meta Platforms Ireland Ltd. (€1.2 billion fine).

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r. 3(2) (India).

The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Kaspersky. (2023). *The state of stalkerware 2022.* Securelist.

Kaspersky. (2024). *The state of stalkerware 2023.* Securelist.

Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122.

Luxembourg CNPD. (2021, July). Decision re Amazon Europe Core S.à r.l. (€746 million fine).

National Crime Records Bureau. (2022). *Crime in India 2022: Statistics.* https://ncrb.gov.in

OECD. (1980). *Guidelines governing the protection of privacy and transborder flows of personal data.*

Online Safety Act 2021 (Cth) pt 6 (Austl.).

Online Safety Act 2023, c. 50, § 188 (U.K.) (amending the Sexual Offences Act 2003, c. 42, § 66B).

Parliamentary Committee on Empowerment of Women. (2026). *Cyber crimes and cyber safety of women* (Fourth Report). Parliament of India.

R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

RBI. (2021). *Master directions on digital payment security controls.*

Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*, 93.

SEBI. (n.d.). *Cyber security and cyber resilience framework.*

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*, 477.

Wang, M. Y. (2023). *Don't believe your eyes: Fighting deepfaked nonconsensual pornography with tort law. University of Chicago Legal Forum*, *2022*, 415.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (CC BY 4.0).