

Original Research Article

Data Privacy Challenges in the Age of Artificial Intelligence: A Study of Privacy Awareness and AI Regulation

Isha Singadiya,¹ Harpreet Kaur²

¹*Research Student, Guru Nanak College of Arts, Science and Commerce, Mumbai, India*

²*Research Guide, Guru Nanak College of Arts, Science and Commerce, Mumbai, India*

Received: 10 September, 2026 | Accepted: 24 September, 2026 | Published: 15 October, 2026

Abstract:

The rapid adoption of Artificial Intelligence (AI) has increased the collection, processing and automated use of personal data. While AI supports innovation, personalization and efficiency, data-intensive AI systems create concerns relating to privacy, consent, transparency, profiling, security, surveillance and individual control. In India, the Digital Personal Data Protection Act, 2023 provides a statutory framework for digital personal data, while the Digital Personal Data Protection Rules, 2025 provide the implementation framework.

This study examines privacy awareness and stakeholder perceptions of data-protection regulation in an AI-driven environment using secondary empirical evidence obtained from an existing published research/data source. The analysis focuses on privacy awareness, awareness of selected rights under the DPDP Act, perceived regulatory effectiveness, privacy-business balance and grievance redressal. Reported statistical evidence indicates higher privacy-awareness scores for professional stakeholders than laypersons, while organizational communication is associated with stronger awareness of privacy rights.

Keywords: Artificial Intelligence, Data Privacy, Privacy Awareness, AI Regulation, DPDP Act 2023, AI Governance, Data Protection, Ethics.

1.0 Introduction

1.1 Artificial Intelligence and Data Privacy

Artificial Intelligence is increasingly used for automated decision-making, personalization, pattern recognition, customer services, healthcare, banking, education, cybersecurity and other applications. The effectiveness of many AI systems depends on large quantities of data, including personal, behavioural and user-generated information.

This close relationship between AI and data creates privacy challenges. Risks may arise through excessive collection, profiling, inference of sensitive information, secondary use, unauthorized disclosure and limited understanding of how AI systems process personal information.

1.2 Indian Legal and Governance Context

India's data-protection framework has developed through the Digital Personal Data Protection Act, 2023. The Act establishes obligations relating to processing of digital personal data and provides rights and responsibilities for individuals and organizations. The Digital Personal Data Protection Rules, 2025 provide the detailed implementation framework.

For AI governance, legislation must be supported by awareness, implementation, transparency and practical mechanisms through which individuals can exercise their rights.

1.3 Privacy Awareness and AI Regulation

Privacy awareness refers to an individual's understanding of personal-data rights, data practices and available privacy protections. In an AI environment, this also includes understanding automated processing, profiling, consent, transparency and grievance mechanisms.

2.0 Problem Statement and Need for the Study

AI systems increasingly operate in data-rich environments in which personal information can be collected and analyzed at scale. This creates a governance challenge: innovation and data-driven services require information, while individuals expect privacy, security, transparency and meaningful control over personal data.

The existence of a data-protection law does not automatically guarantee effective protection. Practical protection also depends on awareness, institutional communication, implementation capability and accessible grievance mechanisms.

3.0 Literature Review

Study	Area	Main contribution	Limitation
Ahmed & Nasir (2026)	India – DPDP Act	Privacy awareness and organizational communication	Stakeholder-specific
Biju & Gayathri (2025)	India – Data rights/AI policy	Data-rights and culture-sensitive governance	Policy/socio-legal focus
Gupta (2026)	India – AI regulation	Bias, opacity and redress challenges	Review-based
Joshi et al. (2026)	AI healthcare	Privacy, security and data protection	Healthcare-specific

Leach et al. (2024)	Responsible AI in India	Privacy, data protection, bias and discrimination	Expert/focus-group perspective
Gupta & Junghare (2026)	India–EU	Privacy-regulation comparison	Legal/comparative focus
Rivera et al. (2026)	Public privacy awareness	IT Act vs DPDP awareness	Limited technical AI focus
Kumaraguru & Sachdeva (2012)	Indian privacy attitudes	Historical privacy-awareness evidence	Before current AI/DPDP
Shrestha et al. (2024)	Youth AI privacy	Data sharing, control and transparency	Youth/international focus
Data Protection in AI Services (2020)	AI privacy	Controls for personalized AI services	Limited Indian evidence

3.1 Research Gap

Although India has substantial policy and legal research relating to AI and data protection, stakeholder-level empirical research remains comparatively limited. The present study therefore focuses on privacy awareness and perceptions of data-protection regulation, while considering professional exposure and organizational communication.

4.0 Objectives, Variables and Hypotheses

- To assess privacy and data-protection awareness.
- To examine whether privacy awareness differs between professional stakeholders and laypersons.
- To examine awareness of selected rights under the DPDP Act, 2023.
- To examine whether organizational communication is associated with stronger privacy-rights awareness.
- To examine perceptions of regulatory effectiveness, privacy-business balance and grievance redressal.
- To provide recommendations for strengthening AI-related privacy governance and awareness.

4.1 Variables

Variable Type	Variable	Role in Study	Operational Focus
Independent Variable	Professional Status	Predictor/ grouping variable	Professional stakeholder vs. layperson
Independent Variable	Organizational Communication	Predictor / contextual variable	Whether information about the DPDP Act was received from an organization/employer
Independent Variable	Privacy Awareness	Predictor variable	Overall understanding of privacy and personal-data practices
Independent Variable	DPDP Rights Awareness	Predictor variable	Awareness of access, correction and erasure rights
Dependent Variable	DPDP Rights Awareness	Outcome variable	Level of awareness of the three examined rights
Dependent Variable	Perceived Regulatory Effectiveness	Outcome variable	Perceived effectiveness of data-protection regulation
Dependent Variable	Privacy-Business Balance	Outcome variable	Perception of balancing privacy with legitimate data-processing needs
Dependent Variable	Grievance Redressal	Outcome variable	Perceived adequacy/effectiveness of grievance mechanisms

The research framework contains four independent variables—professional status, organizational communication, privacy awareness and DPDP-rights awareness—and four dependent variables—DPDP-rights awareness, perceived regulatory effectiveness, privacy-business balance and grievance redressal. The source evidence directly tests selected relationships among these variables; the framework therefore distinguishes predictor and outcome roles for the proposed analysis.

4.2 Hypotheses

Hypothesis	Null (H0)	Alternative (H1)	Test
H1	No significant difference in privacy awareness.	Significant difference in privacy awareness.	Independent-samples t-test
H2	Professional status is independent of rights awareness.	Professional status is associated with rights awareness.	Chi-square
H3	Professional status is independent of privacy-business balance.	Professional status is associated with privacy-business balance.	Chi-square
H4	Professional status is independent of regulatory effectiveness.	Professional status is associated with regulatory effectiveness.	Chi-square

5.0 Methodology

5.1 Research Design

The study adopts a quantitative, explanatory secondary-data research design. A deductive approach is used: concepts identified through the literature are converted into measurable variables and hypotheses, and the reported secondary empirical evidence is analyzed and interpreted in relation to the research objectives.

5.2 Data Source and Data Collection

The study uses secondary data obtained from an existing published research/data source rather than a primary survey conducted by the present researcher. No new questionnaire responses were collected for this research. The analysis is therefore limited to the variables and observations made available through the secondary source.

5.3 Sample / Observation Information

The analysis uses the observations available in the selected secondary dataset/source. The present paper does not present the original source-study respondent count as a newly collected sample, because the researcher did not conduct the survey.

5.4 Statistical Techniques

- Descriptive statistics and percentage analysis
- Independent-samples t-test
- Chi-square test
- Kendall's tau-b
- Effect-size interpretation using Cohen's d

A significance level of 0.05 is used for hypothesis interpretation.

6.0 Data Analysis and Findings

The following figures are based on the numerical findings reported in the secondary source used for this study. They are presented as secondary-data findings and are not presented as results of a primary survey conducted by the researcher.

6.1 Privacy-Awareness Comparison

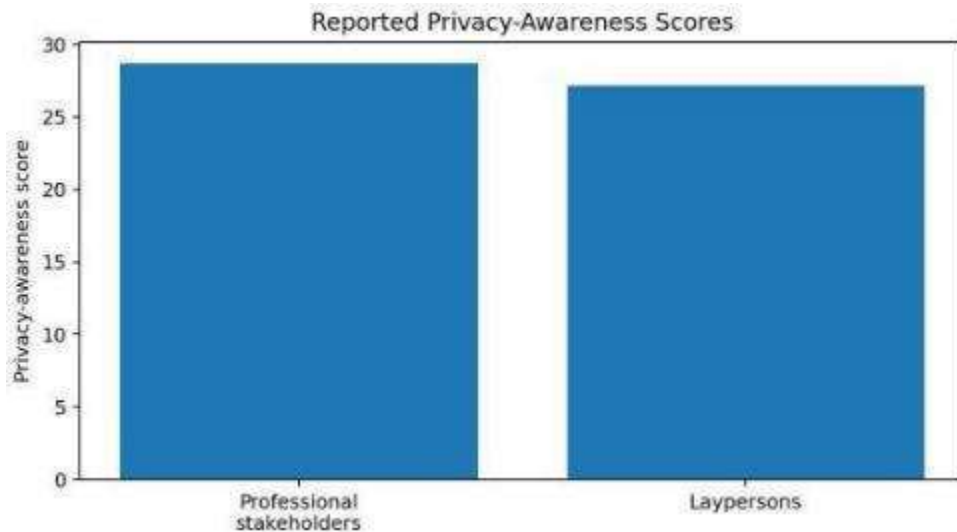


Figure 1. Reported privacy-awareness scores.

The reported mean privacy-awareness score was 28.72 for professional stakeholders and 27.19 for laypersons. The reported independent-samples t-test was statistically significant ($t(378) = 3.40, p = 0.001$). Cohen's $d = 0.34$ indicates a small practical effect.

6.2 Awareness of the Three Examined Privacy Rights

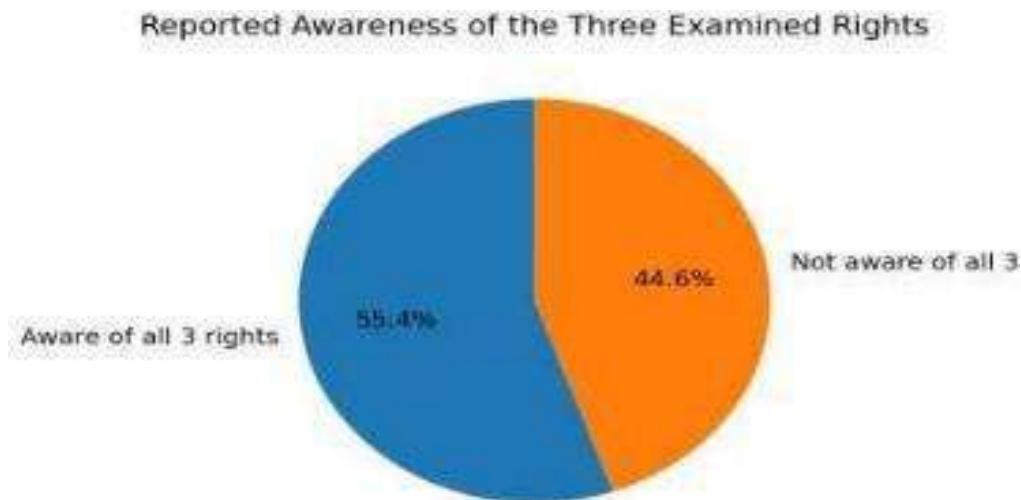


Figure 2. Reported awareness of all three examined rights.

The three examined rights were access, correction and erasure. The reported source result indicates that 55.4% demonstrated awareness of all three rights.

6.3 Organizational Communication and Rights Awareness

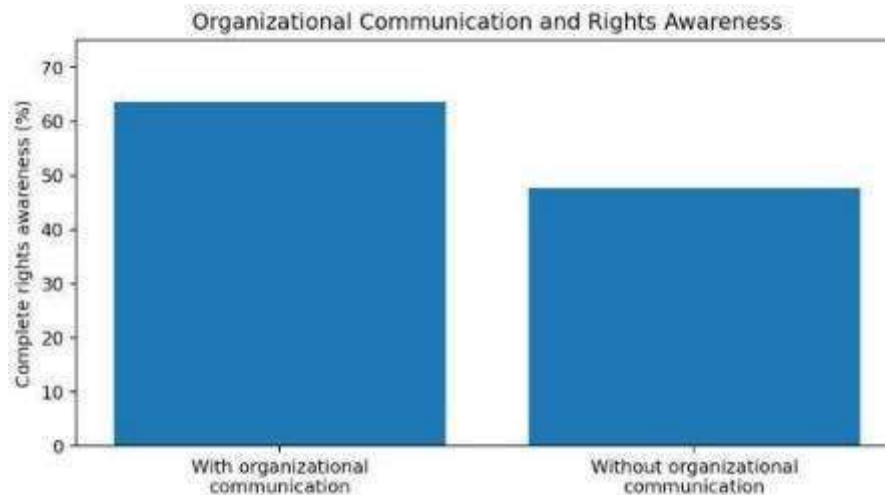


Figure 3. Reported relationship between organizational communication and rights awareness.

Among those who received information about the DPDP Act from an organization, 63.7% demonstrated awareness of all three rights, compared with 47.7% among those who did not receive such information. The reported association was statistically significant ($p = 0.015$).

6.4 Statistical Test Summary

Analysis	Reported p-value	Decision at 0.05	Interpretation
Privacy awareness	0.001	Reject H0	Statistically significant difference
Rights awareness vs professional status	0.152	Fail to reject H0	Not statistically significant
Privacy-business balance	0.074	Fail to reject H0	Not statistically significant
Regulatory effectiveness	0.067	Fail to reject H0	Not statistically significant
Grievance redressal	0.004	Significant	Statistically significant but weak relationship

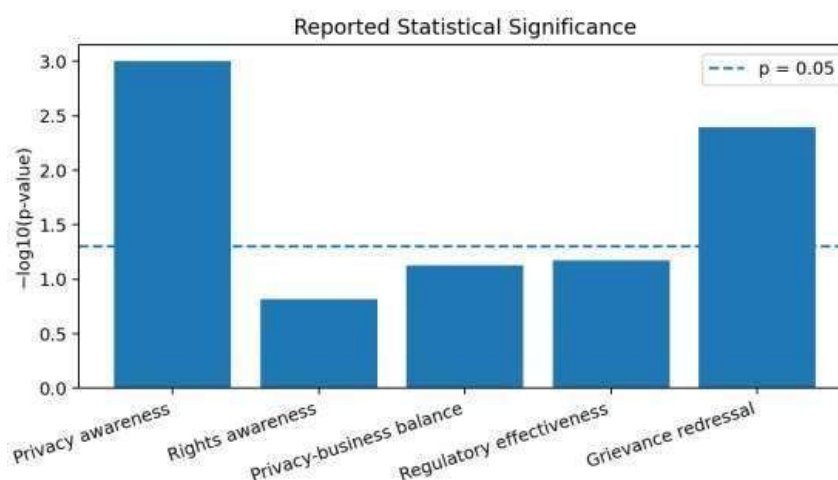


Figure 4. Visual comparison of reported significance levels.

6.5 Interpretation of Findings

The reported findings suggest that professional exposure is associated with somewhat higher privacy awareness, although the practical effect is small. Organizational communication shows a significant association with awareness of privacy rights, supporting the importance of institutional communication for practical privacy literacy.

Professional status was not significantly associated with reported perceptions of regulatory effectiveness or privacy-business balance. The grievance-redressal analysis showed a statistically significant but weak relationship, highlighting the importance of accessible mechanisms for raising and resolving privacy-related concerns.

7.0 Recommendations

- Strengthen privacy-awareness and digital-literacy programmes.
- Improve organizational communication regarding privacy rights and responsibilities.
- Provide clear privacy information to individuals interacting with AI-powered systems.
- Adopt privacy-by-design practices during AI development.
- Improve accessibility and usability of grievance-redressal mechanisms.
- Develop sector-specific AI privacy guidance for banking, healthcare, employment and public services.
- Improve algorithmic transparency where AI systems profile individuals or support automated decisions.
- Regularly evaluate whether users understand and can practically exercise privacy safeguards.
- Adopt proportionate, risk-based AI governance rather than identical requirements for every AI application.

8.0 Conclusion

Artificial Intelligence is increasing the importance and value of personal data while creating new challenges for privacy, transparency, security and responsible governance.

Using secondary empirical evidence, this study examined privacy awareness and stakeholder perceptions of data-protection regulation in an AI-driven environment. The reported evidence indicates a significant difference in privacy-awareness scores between professional stakeholders and laypersons, while the practical effect is small. Awareness of the three examined rights was also associated with organizational communication about the DPDP Act.

The findings suggest that effective AI governance cannot depend on legislation alone. Public awareness, institutional communication, transparent implementation, accessible grievance redressal and continuous evaluation are required to translate privacy principles into practical protection.

9.0 Limitations And Future Scope

The study is based on secondary data and therefore depends on the variables, coding and quality of the original source. The present researcher did not conduct the underlying survey. The findings are also limited to the stakeholder groups and measures available in the selected source.

Future research can use a clearly documented public/Kaggle dataset with reproducible CSV-based analysis, conduct a primary survey for validation, compare demographic groups, and examine privacy risks associated with generative AI, facial recognition and automated decision-making.

10.0 Bibliography

1. Ahmed, S., & Nasir, M. (2026). Stakeholder perceptions of India's Digital Personal Data Protection Act of 2023: An empirical study across legal, banking, and corporate sectors. *Frontiers in Sociology*, 11, 1753383.
2. Biju, P. R., & Gayathri, O. (2025). Indian approach to data rights: Survey of social structures, and personal data protection regimes in India. *International Journal of Electronic Governance*, 17(1), 51–85.
3. Biju, P. R., & Gayathri, O. (2026). Structural oppression and AI: A systematic review of data policy frameworks in India. *Technological Forecasting and Social Change*, 223, 124415.
4. Gupta, S. (2026). India's AI regulation at the crossroads: A comprehensive law or a sectoral mosaic? *Journal of Development Policy and Practice*, 11(1), 120–132.
5. Gupta, T., & Junghare, V. (2026). Privacy and data protection in AI: A comparative analysis of EU and Indian regulatory frameworks. *International Journal of Social Science and Human Research*, 9(2).
6. Joshi, U., Baisil, S., Kini, S. B., Mehta, M., & Datta, S. (2026). AI ethics in Indian healthcare: A scoping review of national and international guidelines on privacy, data protection, and security. *BMC Medical Ethics*, 27, 86.
7. Kumaraguru, P., & Sachdeva, N. (2012). Privacy in India: Attitudes and awareness V 2.0. PreCog Research Group, IIIT-Delhi.
8. Leach, T., et al. (2024). Ensuring a 'Responsible' AI future in India: RRI as an approach for identifying the ethical challenges from an Indian perspective. *AI and Ethics*.
9. Rivera, A. S. S., Dhanmeeswaran, G., & Janarthanan, S. (2026). Awareness Gap Between the IT Act 2000 and the Digital Personal Data Protection Act 2023: A Survey on Data Privacy Challenges in India. *International Journal of Engineering Research & Technology*, 15(6).
10. Shrestha, A. K., et al. (2024). Navigating AI to unpack youth privacy concerns: An in-depth exploration and systematic review. *arXiv*.
11. Data Protection in AI Services: A Survey. (2020). *ACM Computing Surveys*, 54(2).
12. Government of India. (2023). Digital Personal Data Protection Act, 2023.
13. Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025.