Personal Data and Persuasion: Legal Safeguards for Privacy and Consumer Protection in Targeted Advertising under the DPDP Act, 2023

*Suman Mohanty

KIIT School of Law, KIIT Deemed to be University, Bhubaneswar, Odisha, India

advsuman8@gmail.com

Tulishree Pradhan

KIIT School of Law, KIIT Deemed to be University, Bhubaneswar, Odisha, India

Sankalp Sundaray

KIIT School of Law, KIIT Deemed to be University, Bhubaneswar, Odisha, India

Sanghamitra Patnaik

KIIT School of Law, KIIT Deemed to be University, Bhubaneswar, Odisha, India

Pramit Ch. Rout

SOA National Institute of Law, Bhubaneswar, Odisha, India

Abstract. In the digital economy, advertising has shifted from broad messaging to hyper-personalised persuasion, with targeted advertising now standing at the centre of modern marketing. While this data-driven model delivers precision for businesses and convenience for consumers, it also erodes privacy, distorts consent, and exposes individuals to manipulative profiling. In India, this tension has intensified as digital adoption has outpaced the evolution of legal safeguards, leaving consumers vulnerable to data misuse, opaque algorithms, and exploitative practices. The Digital Personal Data Protection (DPDP) Act, 2023 represents a landmark attempt to regulate personal data processing, embedding principles of consent, purpose limitation, accountability, and grievance redress. This paper undertakes a comprehensive legal analysis of targeted advertising under the DPDP Act, examining its provisions against global benchmarks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). It

© The Author(s) 2026

A. Tripathy and K. Mohanty (eds.), *Proceedings of the 5th International Conference on Management Research (ICMR 2025)*, Advances in Economics, Business and Management Research 379,
https://doi.org/10.2991/978-94-6239-660-9_18

identifies critical gaps; such as weak algorithmic accountability, inadequate duties for ad-tech intermediaries, and limited remedies for aggrieved consumers; that dilute the Act's capacity to curb privacy-invasive advertising. To ground this analysis, the study incorporates an empirical component evaluating consumer awareness of data rights and the degree of business compliance with the DPDP framework. The findings reveal low public understanding of data rights and inconsistent adherence by businesses, highlighting the urgent need for stronger enforcement, mandatory transparency standards, and public legal literacy initiatives. By proposing targeted reforms, this paper argues that the DPDP Act can evolve from a narrow privacy statute into a robust legal instrument safeguarding consumer autonomy and ethical advertising in India's data-driven marketplace.

Keywords: Consumer Protection, Digital Economy, Ethical Advertising, GDPR, Privacy, Targeted Advertising.

1. Introduction

1.1 Context and Importance of Targeted Advertising

Targeted advertising has become an indispensable tool in modern marketing, relying on advanced technologies such as artificial intelligence (AI), machine learning (ML), and data analytics to deliver highly personalized consumer experiences. This paradigm shift has enabled businesses to enhance engagement and operational efficiency, driving significant growth in digital marketing (Tucker, 2014). However, the extensive collection and utilization of personal data inherent in these practices have precipitated significant legal and ethical concerns, particularly regarding individual privacy and consumer rights (Acquisti, Taylor, & Wagman, 2016).

In India, the rapid digital transformation and the proliferation of e-commerce platforms have accelerated the adoption of targeted advertising. However, this progression has often outpaced the establishment of comprehensive data protection frameworks, exposing consumers to potential data misuse and privacy infringements (Gupta, 2023). The **Digital Personal Data Protection (DPDP) Act, 2023**, represents a critical legislative advancement aimed at addressing these challenges by instituting robust safeguards centered on transparency, accountability, and informed consent (Ministry of Electronics and Information Technology, 2023).

1.2 Privacy Concerns in the Digital Era

The right to privacy is universally regarded as fundamental and enshrined in various international and domestic legal frameworks. In India, the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) affirmed privacy as intrinsic to the right to life and personal liberty under Article 21 of the Constitution (Supreme Court Observer, 2017). Despite this recognition, the digital ecosystem presents unprecedented challenges, as businesses exploit consumer data for profit without adequate safeguards (Nair, 2022).

Targeted advertising epitomizes these challenges, often involving invasive tracking of user behavior, preferences, and demographics. While economically advantageous, such practices blur ethical boundaries concerning data collection and processing (Shah & Patel, 2023). The DPDP Act seeks to mitigate these issues by introducing stringent consent requirements, restricting data retention, and imposing penalties for non-compliance (Ministry of Electronics and Information Technology, 2023).

1.3 Objectives and Scope of the Study

- This study undertakes a critical examination of the regulatory framework governing targeted advertising in India under the Digital Personal Data Protection (DPDP) Act, 2023, with particular emphasis on its implications for consumer privacy and data autonomy. It interrogates the extent to which the DPDP Act addresses issues such as informed consent, purpose limitation, data minimisation, profiling restrictions, and grievance redressal in the context of algorithm-driven targeted advertising.

- To contextualise India's framework, the paper juxtaposes it with leading global data protection regimes, notably the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA), both of which have established greatest standards on data subject rights, opt-out mechanisms, transparency mandates, and enforcement architecture. This comparative lens seeks to identify key regulatory gaps and ambiguities within the Indian regime, including weak consent standards, absence of explicit rules on algorithmic profiling and behavioural tracking, limited independent oversight, and inadequate penalties for non-compliance.

- It further explores the institutional and infrastructural challenges of enforcement, such as capacity constraints of the Data Protection Board, cross-border data transfer complexities, and the difficulties of auditing opaque ad-tech ecosystems. Ultimately, the paper aims to propose policy and legislative measures to harmonise technological innovation in digital advertising with ethical and privacy-preserving practices, thereby ensuring that economic efficiency does not come at the cost of individual rights and informational self-determination (Greenleaf, 2022).

1.4 Methodology Overview

Employing a mixed-methods approach, this study integrates doctrinal legal analysis with empirical research. The doctrinal component entails a meticulous examination of statutory provisions, judicial interpretations, and comparative legal frameworks. Concurrently, the empirical component assesses consumer awareness and industry

compliance with the DPDP Act, providing a nuanced understanding of the interplay between law, technology, and consumer protection (Mitra, 2023).

1.5 Structure of the Paper

The paper is structured into eight sections. This introductory section establishes the context and objectives of the study. Section 2 elucidates the mechanisms and practices underlying targeted advertising. Section 3 examines the legal and ethical concerns associated with these practices. Section 4 offers a detailed analysis of the DPDP Act, 2023. Section 5 presents empirical findings on consumer awareness and compliance. Section 6 explores enforcement challenges and regulatory gaps. Section 7 provides recommendations for policymakers and stakeholders. Finally, Section 8 concludes with key insights and directions for future research.

2. Targeted Advertising: Concept and Mechanisms

2.1 Definition and Evolution

Targeted advertising refers to the practice of delivering personalized promotional content to consumers based on their behaviours, preferences, and demographic profiles. It marks a departure from traditional advertising approaches, which rely on broader audience targeting with limited personalization. This shift was catalysed by advancements in digital technology, enabling advertisers to harness user data for refined audience segmentation (Goldfarb & Tucker, 2011). The proliferation of e-commerce and social media platforms has further accelerated this transformation, embedding targeted advertising as a cornerstone of modern marketing strategies.

Historically, targeted advertising evolved from basic contextual advertising, where ads were aligned with website content, to sophisticated behavioural targeting models. Platforms now integrate artificial intelligence (AI) and machine learning (ML) to analyse user data, predict preferences, and serve tailored ads in real-time (Chen et al., 2021). The evolution underscores a growing reliance on consumer data, often collected through cookies, web tracking technologies, and voluntary inputs such as search queries.

2.2 Key Technologies Enabling Targeted Advertising

The mechanics of targeted advertising are underpinned by cutting-edge technologies designed to optimize user engagement:

- **Cookies and Web Beacons:** These tools enable platforms to track user behavior across websites, collecting information on browsing history and click-through rates (Shields & Pasternack, 2022).

- **Programmatic Advertising:** This automated system leverages algorithms to purchase ad space, ensuring precise targeting based on real-time bidding (RTB) and data analytics (Mehta et al., 2020).
- **Artificial Intelligence and Machine Learning:** These technologies analyse vast datasets to predict consumer preferences, enabling hyper-personalized ad placements (Chen et al., 2021).
- **Social Media Analytics:** Platforms such as Facebook and Instagram use proprietary algorithms to deliver ads tailored to user interactions, including likes, shares, and comments (Kaplan & Haenlein, 2019).

2.3 Benefits of Targeted Advertising for Businesses

For businesses, targeted advertising offers unparalleled advantages:

- **Increased Efficiency:** Personalized ads improve conversion rates by focusing on consumers most likely to engage with the product or service (Tucker, 2014).
- **Enhanced Consumer Insights:** By analysing data, businesses gain a deeper understanding of consumer behavior, enabling strategic decision-making (Shah & Verma, 2022).
- **Cost Optimization:** Targeted campaigns reduce wasteful spending by minimizing irrelevant ad impressions, thereby maximizing return on investment (ROI) (Goldfarb & Tucker, 2011).
- **Real-Time Adaptability:** Technologies such as programmatic advertising allow businesses to dynamically adjust campaigns based on performance metrics (Mehta et al., 2020).

2.4 Risks and Challenges for Consumers

Despite its benefits, targeted advertising raises significant risks for consumers:

- **Privacy Infringement:** The collection and processing of personal data often occur without explicit consumer consent, contravening privacy principles (Acquisti et al., 2016).

- **Algorithmic Bias:** Automated systems can reinforce societal biases, leading to discriminatory outcomes in ad placements (Shields & Pasternack, 2022).
- **Data Security Risks:** The extensive data involved in targeted advertising makes platforms vulnerable to breaches, exposing sensitive consumer information (Chen et al., 2021).
- **Erosion of Consumer Autonomy:** The predictive nature of targeted ads can influence consumer choices, raising ethical concerns about manipulation (Kaplan & Haenlein, 2019).

2.5 Legal and Regulatory Considerations

The legal landscape for targeted advertising has become increasingly complex as governments introduce stringent data protection regulations. In India, the **Digital Personal Data Protection (DPDP) Act, 2023**, mandates informed consent for data collection and restricts the processing of personal data for targeted advertising (Ministry of Electronics and Information Technology, 2023). Comparatively, international frameworks such as the **General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act (CCPA)** impose obligations on businesses to ensure transparency, accountability, and data minimization (Greenleaf, 2022).

3. Legal and Ethical Concerns in Targeted Advertising

3.1 Defining Privacy and Consumer Protection

Privacy is widely regarded as a fundamental human right and is protected under various national and international legal frameworks. In India, the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017) firmly established privacy as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution (Supreme Court Observer, 2017). Similarly, international instruments such as the **General Data Protection Regulation (GDPR)** emphasize the protection of personal data and individual autonomy (European Union, 2016).

Consumer protection, on the other hand, seeks to safeguard individuals from unfair trade practices, ensuring that businesses operate with transparency and accountability. In the realm of targeted advertising, this principle is challenged by practices that exploit consumer data without adequate safeguards, often breaching privacy and undermining consumer trust (Greenleaf, 2022).

3.2 Ethical Implications of Data Collection

The ethical challenges of targeted advertising stem largely from the collection and processing of consumer data. One primary concern is the lack of meaningful consent, as consumers are often unaware of the extent to which their data is collected and used. Studies have shown that many privacy policies are overly complex, deterring consumers from fully understanding their rights (Acquisti et al., 2016).

Another pressing issue is algorithmic bias. Targeted advertising algorithms can inadvertently reinforce societal biases, leading to discriminatory outcomes. For instance, advertisements for high-paying jobs may disproportionately target certain demographics while excluding others, raising concerns about fairness and equality (Shah & Patel, 2023).

3.3 The Role of Transparency and Consent

Transparency and consent are foundational to ethical advertising practices. Informed consent ensures that consumers have control over their personal data and understand how it will be used. The **Digital Personal Data Protection (DPDP) Act, 2023**, mandates businesses to obtain explicit consent before collecting or processing personal data. It further requires organizations to provide clear and accessible privacy notices, empowering consumers to make informed decisions (Ministry of Electronics and Information Technology, 2023).

Globally, frameworks like the GDPR have set benchmarks for transparency, requiring businesses to disclose the purposes of data collection and processing. These frameworks not only enhance consumer trust but also hold organizations accountable for their data practices (European Union, 2016).

3.4 Risks of Targeted Advertising

While targeted advertising offers significant economic benefits, it also poses several risks to consumers:

- **Intrusiveness and Behavioural Manipulation:** Personalized ads can intrude upon a consumer's digital space, creating discomfort and diminishing user autonomy. For example, constant exposure to ads based on previous searches can lead to perceived manipulation (Tucker, 2014).
- **Data Breaches:** The extensive data collected for targeted advertising makes businesses prime targets for cyberattacks. Data breaches not only compromise sensitive consumer information but also erode trust in digital platforms (Chen et al., 2021).
- **Erosion of Privacy:** Targeted advertising often blurs the line between acceptable data usage and invasive surveillance. Practices such as cross-platform

tracking exacerbate privacy concerns, as consumers are monitored across multiple digital ecosystems without their explicit knowledge (Shields & Pasternack, 2022).

4. The Digital Personal Data Protection (DPDP) Act, 2023

4.1 Overview of Key Provisions

The **Digital Personal Data Protection (DPDP) Act, 2023**, represents a landmark in India's legislative efforts to regulate the collection, processing, and storage of personal data. It is grounded in principles of transparency, accountability, and informed consent, aligning with global trends in data protection. The Act applies to both government and private entities involved in data processing, extending its jurisdiction to organizations operating outside India if they process the personal data of Indian citizens (Ministry of Electronics and Information Technology, 2023).

Key provisions of the DPDP Act include:

- **Informed Consent:** Data fiduciaries must obtain clear and explicit consent from individuals before processing their personal data. Consent should be freely given, specific, and capable of being withdrawn (Section 7).
- **Purpose Limitation:** Data processing is restricted to purposes explicitly stated at the time of consent, reducing the scope for misuse (Section 5).
- **Accountability of Data Fiduciaries:** Fiduciaries are required to implement organizational measures, such as data audits and privacy impact assessments, to ensure compliance (Section 10).
- **Penalties for Non-Compliance:** The Act imposes steep financial penalties for violations, with fines reaching up to ₹250 crore for data breaches (Section 25).

4.2 Relevance to Targeted Advertising

Targeted advertising, which relies heavily on the collection and analysis of consumer data, is directly impacted by the DPDP Act. The requirement for informed consent before collecting personal data significantly curtails practices such as implicit tracking and data sharing without user knowledge (Gupta, 2023).

For businesses engaging in targeted advertising, the Act introduces several obligations:

- **Data Minimization:** Collect only the data necessary for the specified purpose (Section 6).

- **Data Security:** Implement robust measures to prevent unauthorized access or breaches (Section 8).
- **Transparency Obligations:** Businesses must disclose their data practices to users through clear and accessible privacy notices (Section 12).

4.3 Comparison with Global Frameworks

The DPDP Act draws inspiration from international data protection frameworks, including the **General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act (CCPA)**, while incorporating provisions tailored to India's socio-economic context.

General Data Protection Regulation (GDPR):

- Both the GDPR and DPDP Act emphasize informed consent, data minimization, and accountability. However, the GDPR's scope is broader, with additional requirements for lawful processing bases such as legitimate interests and performance of contracts (European Union, 2016).
- GDPR's extraterritorial application is more explicit, covering data controllers and processors worldwide if they target EU residents.

California Consumer Privacy Act (CCPA):

- The CCPA focuses on granting consumers rights over their data, such as the right to opt-out of data sales. In contrast, the DPDP Act centres on informed consent and penalties for misuse (Greenleaf, 2022).
- Enforcement mechanisms under the CCPA include private rights of action for data breaches, whereas the DPDP Act does not extend similar rights to individuals.

4.4 Enforcement Mechanisms

The DPDP Act establishes the **Data Protection Board of India (DPBI)** as the regulatory authority responsible for enforcing its provisions. The Board is empowered to:

- Investigate complaints related to data breaches or misuse.
- Impose penalties for non-compliance.

- Provide redressal mechanisms for grievances (Ministry of Electronics and Information Technology, 2023).

Despite its robust framework, the Act has faced criticism for granting the government broad exemptions under Section 18, raising concerns about its impartiality and effectiveness in protecting citizen privacy (Nair, 2022).

5. Empirical Analysis

5.1 Demographics of Respondents

Table 1: Gender Distribution of Respondents

Gender	Number of Respondents	Percentage (%)
Male	145	51.1
Female	132	46.5
Non-binary	7	2.5

(Source: Author's own)

The gender distribution indicates a balanced sample, with 51.1% male and 46.5% female respondents. This balance ensures diverse perspectives in the analysis, reflecting how targeted advertising practices may affect different gender groups. The inclusion of non-binary respondents, while small at 2.5%, highlights the study's inclusivity. Gender representation is significant, as prior research suggests that privacy concerns and perceptions of targeted advertising often vary across genders, with women generally reporting greater unease regarding data collection practices.

Table 2: Age Group Distribution

Age Group	Number of Respondents	Percentage (%)
18–25 years	79	27.8
26–35 years	124	43.7
36–45 years	58	20.4
Above 45 years	23	8.1

(Source: Author's own)

The age distribution reveals that the majority of respondents (43.7%) belong to the 26–35 age group, followed by 18–25-year-olds (27.8%). These groups represent tech-savvy generations, frequently interacting with digital platforms where targeted advertising is prevalent. The smaller representation of individuals above 45 years (8.1%)

reflects reduced engagement with digital technologies among older populations. These variations highlight the importance of tailoring privacy education and advertising practices to the digital fluency of different age groups.

Table 3: Education Level of Respondents

Education Level	Number of Respondents	Percentage (%)
Undergraduate	91	32.0
Postgraduate	158	55.6
Doctorate	35	12.3

(Source: Author's own)

Most respondents (55.6%) have completed postgraduate education, suggesting a sample with higher levels of awareness and critical thinking regarding privacy concerns. This demographic is more likely to engage with the nuances of data protection policies, such as the DPDP Act. However, 32% of respondents with undergraduate qualifications and 12.3% with doctorates ensure diverse educational perspectives. The findings imply that privacy-related educational campaigns could target less educated groups to bridge potential awareness gaps.

Table 4: Employment Status

Employment Status	Number of Respondents	Percentage (%)
Employed	202	71.1
Self-employed	41	14.4
Unemployed	41	14.4

(Source: Author's own)

The data shows that 71.1% of respondents are employed, reflecting a population that actively engages with digital platforms for work and consumption. Self-employed and unemployed respondents, both at 14.4%, bring additional viewpoints, particularly concerning trust in online platforms and targeted advertising. Employed respondents are more likely to encounter targeted ads through workplace devices, underscoring the need for workplace data privacy initiatives. The presence of unemployed individuals highlights issues of inclusivity and fairness in targeted advertising practices.

Table 5: Awareness of the Digital Personal Data Protection (DPDP) Act, 2023

Awareness Level	Number of Respondents	Percentage (%)
Fully aware	47	16.5
Partially aware	118	41.5

Not aware	119	42.0

(Source: Author's own)

Awareness levels of the DPDP Act remain low, with only 16.5% of respondents fully aware of its provisions. Partial awareness (41.5%) indicates some familiarity, though insufficient to empower consumers to exercise their rights. The 42% who are unaware entirely highlights the critical need for public education campaigns. Low awareness poses significant barriers to the enforcement of data protection rights, as uninformed consumers are less likely to hold businesses accountable or report violations.

Table 6: Knowledge of Data Collection Practices by Businesses

Data Collection Awareness	Number of Respondents	Percentage (%)
Fully aware	62	21.8
Somewhat aware	132	46.5
Not aware	90	31.7

(Source: Author's own)

The analysis reveals that while 21.8% of respondents are fully aware of data collection practices, a significant portion (46.5%) remains only somewhat informed. This limited awareness often translates into an inability to provide informed consent or challenge inappropriate data usage. The 31.7% of respondents who are entirely unaware of these practices represent a vulnerable segment, underscoring the importance of transparency from businesses and consumer education initiatives.

Table 7: Consumer Sentiments on Targeted Advertising

Sentiment	Number of Respondents	Percentage (%)
Positive	85	29.9
Neutral	120	42.3
Negative	79	27.8

(Source: Author's own)

Consumer sentiments toward targeted advertising reveal a mixed response. Approximately 30% view it positively, highlighting the benefits of personalization and relevance. However, 27.8% express negative sentiments, citing concerns over privacy and perceived intrusiveness. The majority, at 42.3%, remain neutral, potentially indicating

a lack of strong opinions or deeper understanding of the implications of targeted advertising. These findings suggest that businesses need to balance personalization with transparency to address consumer apprehensions.

Table 8: Trust in Businesses Handling Personal Data

Trust Level	Number of Respondents	Percentage (%)
High	40	14.1
Moderate	124	43.7
Low	120	42.3

(Source: Author's own)

The data highlights a significant trust deficit, with only 14.1% of respondents exhibiting high trust in businesses handling personal data. The majority (43.7%) demonstrate moderate trust, while 42.3% report low trust. This indicates a need for businesses to adopt more transparent data handling practices and build trust through compliance with data protection laws. Enhanced consumer awareness of privacy rights under the DPDP Act could further bolster trust.

Table 9: Perceived Adherence to Consent Requirements

Compliance Level	Number of Respondents	Percentage (%)
Always compliant	38	13.4
Sometimes compliant	155	54.6
Rarely compliant	91	32.0

(Source: Author's own)

Perceived adherence to consent requirements by businesses is alarmingly low. Only 13.4% of respondents believe that businesses always comply with consent mandates, while 54.6% perceive sporadic compliance. The remaining 32% believe businesses rarely follow consent protocols. This highlights significant gaps in regulatory adherence and calls for stronger enforcement mechanisms under the DPDP Act to protect consumer rights effectively.

Table 10: Concerns About Data Breaches

Level of Concern	Number of Respondents	Percentage (%)
Very concerned	164	57.7
Somewhat concerned	91	32.0
Not concerned	29	10.2

(Source: Author's own)

A majority of respondents (57.7%) express significant concern about data breaches, reflecting widespread apprehension about the security of personal information. With 32% somewhat concerned and 10.2% unconcerned, the findings underline the need for businesses to prioritize robust data protection measures. These concerns also emphasize the role of regulatory oversight in mitigating risks associated with data breaches.

Table 11: Preferred Communication of Privacy Policies

Communication Method	Number of Respondents	Percentage (%)
Simplified summaries	167	58.8
Full detailed policies	85	29.9
Video or visual formats	32	11.3

(Source: Author's own)

The data shows that consumers overwhelmingly prefer simplified summaries of privacy policies (58.8%) over detailed legal documents (29.9%). This preference suggests that businesses should focus on making privacy information more accessible and comprehensible. Video or visual formats, preferred by 11.3%, highlight an emerging trend toward engaging and user-friendly communication methods.

Table 12: Expectations of Regulatory Enforcement

Enforcement Expectation	Number of Respondents	Percentage (%)
Strict and proactive	201	70.8
Moderate	65	22.9
Minimal	18	6.3

(Source: Author's own)

The overwhelming majority of respondents (70.8%) advocate for strict and proactive enforcement of privacy laws, reflecting a strong desire for accountability in data handling. Moderate expectations (22.9%) and minimal expectations (6.3%) indicate varying levels of trust in the government and regulatory bodies. These results reinforce the urgency for the Data Protection Board of India to act decisively in implementing the DPDP Act.

Table 13: Frequency of Receiving Targeted Ads

Frequency	Number of Respondents	Percentage (%)
Daily	183	64.4
Weekly	71	25.0
Rarely	30	10.6

(Source: Author's own)

The majority of respondents (64.4%) report encountering targeted ads daily, indicating the pervasive nature of this marketing strategy. A significant portion (25%) receives ads weekly, while 10.6% rarely experience them. These findings highlight the high visibility of targeted advertising and underscore the necessity for businesses to align their strategies with ethical and legal standards, as frequent exposure could increase consumer sensitivity to privacy violations.

Table 14: Intrusiveness of Targeted Ads

Level of Intrusiveness	Number of Respondents	Percentage (%)
Highly intrusive	110	38.7
Somewhat intrusive	128	45.1
Not intrusive	46	16.2

(Source: Author's own)

Over 83% of respondents perceive targeted ads as intrusive, with 38.7% describing them as highly intrusive. Only 16.2% find them unobtrusive. These results underscore consumer discomfort, emphasizing the need for businesses to adopt less invasive techniques. Transparency in data usage and clearer consent mechanisms could mitigate perceptions of intrusiveness.

Table 15: Awareness of Retargeting Practices

Awareness Level	Number of Respondents	Percentage (%)
Fully aware	68	23.9
Somewhat aware	144	50.7
Not aware	72	25.4

(Source: Author's own)

The data reveals that 50.7% of respondents are somewhat aware of retargeting practices, while only 23.9% are fully aware. Retargeting, a common advertising strategy, is

often perceived as invasive due to its visibility. The 25.4% who are unaware of these practices further demonstrate the need for consumer education and greater transparency in explaining advertising mechanisms.

Table 16: Concerns About Sharing Data with Third Parties

Level of Concern	Number of Respondents	Percentage (%)
Very concerned	176	62.0
Somewhat concerned	89	31.3
Not concerned	19	6.7

(Source: Author's own)

A substantial 62% of respondents express significant concern over data sharing with third parties, highlighting consumer apprehensions about transparency and control. The 31.3% who are somewhat concerned suggest varying degrees of trust in data practices. Businesses must address these concerns by clearly outlining third-party data-sharing policies and obtaining explicit consent.

Table 17: Satisfaction with Existing Privacy Controls

Satisfaction Level	Number of Respondents	Percentage (%)
Very satisfied	54	19.0
Somewhat satisfied	143	50.4
Dissatisfied	87	30.6

(Source: Author's own)

While 50.4% of respondents are somewhat satisfied with existing privacy controls, 30.6% express dissatisfaction, reflecting unmet consumer expectations. Only 19% are highly satisfied, pointing to a pressing need for more robust privacy features and clear communication from businesses about data usage.

Table 18: Preference for Opt-Out Mechanisms

Preference Level	Number of Respondents	Percentage (%)
Strongly prefer	189	66.5
Neutral	76	26.8
Not interested	19	6.7

(Source: Author's own)

Most respondents (66.5%) strongly prefer opt-out mechanisms for targeted advertising, indicating a demand for greater control over data usage. Neutral responses (26.8%) suggest indifference or a lack of awareness about such options. Businesses should prioritize user-friendly opt-out features to enhance consumer satisfaction and compliance with regulations.

Table 19: Trust in Regulatory Bodies

Trust Level	Number of Respondents	Percentage (%)
High trust	77	27.1
Moderate trust	145	51.1
Low trust	62	21.8

(Source: Author's own)

The majority (51.1%) of respondents exhibit moderate trust in regulatory bodies, reflecting cautious optimism regarding enforcement of privacy laws. However, 21.8% report low trust, suggesting scepticism about the effectiveness of regulatory actions. These findings underscore the need for visible, proactive enforcement measures by authorities to build consumer confidence.

Table 20: Perceived Benefits of Targeted Advertising

Benefit	Number of Respondents	Percentage (%)
Relevant product suggestions	154	54.2
Time-saving in decision-making	89	31.3
Enhanced shopping experience	41	14.5

(Source: Author's own)

The majority of respondents (54.2%) perceive targeted advertising as beneficial due to its relevance in suggesting products that align with their preferences. Another 31.3% appreciate the time-saving aspect in decision-making. However, only 14.5% report enhanced shopping experiences. These insights suggest that while targeted advertising offers utility, its perceived advantages remain limited and may not outweigh privacy concerns for many consumers.

Table 21: Perceived Risks of Targeted Advertising

Risk	Number of Respondents	Percentage (%)
Privacy invasion	174	61.3
Data misuse	81	28.5
Over-personalization	29	10.2

(Source: Author's own)

Privacy invasion is the most significant concern, cited by 61.3% of respondents. Data misuse (28.5%) also ranks high, indicating apprehensions about the lack of control over personal information. Over-personalization (10.2%) is a lesser concern but still highlights discomfort with overly tailored advertisements. These findings emphasize the need for businesses to address these risks transparently and ethically.

Table 22: Willingness to Pay for Ad-Free Experiences

Willingness Level	Number of Respondents	Percentage (%)
Willing	107	37.7
Neutral	94	33.1
Unwilling	83	29.2

(Source: Author's own)

A substantial 37.7% of respondents express a willingness to pay for ad-free experiences, reflecting a preference for privacy over free, ad-supported services. The neutral stance of 33.1% suggests that many consumers are undecided, while 29.2% remain unwilling to pay. These findings could guide businesses in exploring premium models that balance privacy and revenue.

Table 23: Preference for Data Minimization Practices

Preference Level	Number of Respondents	Percentage (%)
Strongly prefer	204	71.8
Neutral	64	22.5
Not interested	16	5.6

(Source: Author's own)

Most respondents (71.8%) strongly favour data minimization practices, emphasizing the importance of collecting only essential data for specified purposes. Neutral responses (22.5%) indicate some indifference, while a small minority (5.6%) are not interested. These results underscore the necessity for businesses to prioritize minimal data collection in compliance with privacy regulations.

Table 24: Expectations of Transparency from Businesses

Transparency Expectation	Number of Respondents	Percentage (%)
High transparency	214	75.4
Moderate transparency	56	19.7
Low transparency	14	4.9

(Source: Author's own)

The overwhelming majority (75.4%) expect high transparency from businesses regarding their data practices. Moderate transparency expectations (19.7%) suggest varying degrees of trust, while only 4.9% express low expectations. This highlights the critical role of clear and accessible communication in fostering consumer trust and aligning with data protection norms.

Table 25: Likelihood of Reporting Data Misuse

Likelihood	Number of Respondents	Percentage (%)
Very likely	181	63.7
Somewhat likely	79	27.8
Unlikely	24	8.5

(Source: Author's own)

A strong majority (63.7%) are very likely to report cases of data misuse, reflecting growing consumer awareness and a willingness to hold businesses accountable. Another 27.8% are somewhat likely, while only 8.5% are unlikely to take action. These results underline the importance of accessible reporting mechanisms and consumer empowerment initiatives under the DPDP Act.

6. Empirical Analysis – Qualitative Insights

In addition to the quantitative findings, qualitative insights were gathered through open-ended survey responses from the sample of 284 participants. These responses provide deeper perspectives on consumer concerns, perceptions, and expectations regarding targeted advertising and data protection under the DPDP Act.

6.1 Qualitative Themes

- **Consumer Concerns about Privacy** Participants consistently expressed anxiety about how businesses handle their data. A respondent commented:

"I often feel like my online behavior is monitored excessively. It's unsettling to receive ads about something I casually searched for just once."

This sentiment reflects a broader discomfort with the perceived lack of transparency in data collection practices. Many participants highlighted the intrusive nature of targeted advertising and a desire for stricter enforcement of consent requirements.

- **Expectations from Businesses** A recurring theme in the qualitative responses was the demand for more control over personal data. As one participant noted:
  "I want businesses to give me clearer options to opt-out of data sharing. Privacy policies should be easy to understand, not pages of legal jargon."
  This underscores the need for user-friendly privacy controls and simplified communication of data practices.
- **Perceived Benefits and Ethical Dilemmas** While many respondents acknowledged the convenience of personalized ads, they questioned the ethical trade-offs. One individual stated:
  "I appreciate when ads are relevant, but it feels like the cost of personalization is losing control over my own information."
  This highlights the tension between consumer convenience and privacy, emphasizing the ethical dilemmas inherent in targeted advertising.
- **Data Breaches and Accountability** Respondents voiced strong concerns about the security of their data, particularly in light of high-profile data breaches. A participant shared:
  "Businesses are quick to collect my data but slow to take responsibility when there's a breach. I feel helpless when my information is compromised."
  This emphasizes the importance of accountability mechanisms and consumer trust-building measures.
- **Awareness of the DPDP Act** A significant number of respondents indicated limited knowledge of the DPDP Act but expressed optimism about its potential impact:
  "If implemented properly, the DPDP Act could be a game-changer. But for now, I don't see much difference in how businesses operate."

This reflects both hope and scepticism about the enforcement of the Act and its ability to regulate data practices effectively.

6.2. Challenges in Implementation and Enforcement

Regulatory Gaps and Challenges

The **Digital Personal Data Protection (DPDP) Act, 2023** has been hailed as a transformative step in India's data protection regime. However, it faces criticism for several loopholes that undermine its objectives. One major challenge lies in the **broad exemptions granted to the government** under Section 18 of the Act. These exemptions allow public authorities to bypass certain compliance requirements in the interest of national security or public order, raising concerns about potential misuse and selective enforcement (Gupta, 2023).

Additionally, the Act lacks clarity on key provisions such as the definition of "significant data fiduciaries" and the criteria for imposing compliance obligations. Ambiguities in interpretation may lead to inconsistent application, creating loopholes for businesses to evade stringent requirements (Greenleaf, 2022). This regulatory opacity weakens the Act's potential to establish a robust data protection framework.

Practical Challenges for Businesses

For businesses, implementing the DPDP Act poses significant logistical and financial hurdles. Many small and medium enterprises (SMEs) lack the infrastructure to comply with the Act's stringent requirements, such as conducting **privacy impact assessments** and ensuring real-time monitoring of data processing activities (Mitra, 2023). The cost of compliance, including investments in technology, training, and legal advisory services, may disproportionately burden smaller organizations.

Balancing personalization and privacy is another challenge. Businesses relying on targeted advertising must reconfigure their data collection and processing mechanisms to align with the Act's consent and minimization principles. These adjustments may dilute the effectiveness of their marketing strategies, forcing businesses to reconsider their value propositions.

Enforcement Mechanisms

The establishment of the **Data Protection Board of India (DPBI)** is a cornerstone of the DPDP Act's enforcement framework. Tasked with addressing complaints, conducting investigations, and imposing penalties, the DPBI holds significant responsibilities (Ministry of Electronics and Information Technology, 2023). However, the Board's effectiveness is hindered by potential resource constraints, lack of autonomy, and the absence of granular enforcement guidelines.

For instance, the Act does not provide mechanisms for proactive audits of data fiduciaries, relying instead on consumer complaints to trigger enforcement actions. This reactive approach limits the Board's ability to prompt violations, potentially undermining the overall deterrent effect of the law (Nair, 2022).

Consumer-Centric Challenges

Consumers are pivotal to the enforcement of the DPDP Act, as their complaints often initiate regulatory actions. However, **low awareness levels** regarding data protection rights significantly impede enforcement efforts. As revealed in Section 5, 42% of respondents were unaware of the DPDP Act, and many others lacked clarity on how to exercise their rights effectively.

Moreover, even aware consumers may hesitate to report violations due to concerns about retaliation, lack of trust in enforcement mechanisms, or the perception that their complaints will not result in meaningful action (Shah & Patel, 2023). Addressing these challenges requires sustained public education campaigns and simplified reporting mechanisms to empower consumers.

Balancing Innovation with Privacy

The digital economy thrives on innovation, often fueled by the use of personal data. Striking a balance between fostering technological advancements and safeguarding consumer privacy presents a broader challenge for policymakers. Overly stringent regulations may stifle innovation, particularly for startups and SMEs, while lenient enforcement could erode consumer trust (Tucker, 2014). This delicate equilibrium demands nuanced policymaking and iterative regulatory frameworks that adapt to emerging technological trends.

7. Recommendations for Policy and Practice

7.1 Enhancing Public Awareness

One of the foundational challenges in enforcing the **Digital Personal Data Protection (DPDP) Act, 2023**, is the widespread lack of consumer awareness about privacy rights and data protection mechanisms. Public education campaigns are crucial to address this gap. The government, in collaboration with civil society organizations, should conduct nationwide outreach programs using multimedia platforms to explain the Act's key provisions in simple terms (Gupta, 2023).

Businesses must also simplify their privacy policies and consent forms to make them comprehensible for the average user. Leveraging visual aids, videos, and interactive content can help consumers make informed decisions about their data usage (Greenleaf, 2022). A standardized privacy notice format, similar to GDPR's guidelines, could ensure consistency and ease of understanding.

7.2 Strengthening Regulatory Oversight

To ensure effective enforcement, the **Data Protection Board of India (DPBI)** must be empowered with greater resources and autonomy. Proactive auditing mechanisms should be introduced, allowing the DPBI to regularly assess compliance by data fiduciaries, rather than relying solely on consumer complaints (Ministry of Electronics and Information Technology, 2023).

The introduction of sector-specific guidelines tailored to industries like e-commerce, healthcare, and finance could help bridge regulatory gaps. Additionally, penalties for non-compliance should be tiered based on the severity of violations, ensuring proportionality and encouraging corrective actions rather than punitive measures alone (Nair, 2022).

7.3 Encouraging Business Compliance

Adopting privacy-friendly practices can be resource-intensive, particularly for small and medium enterprises (SMEs). The government should consider offering incentives, such as tax breaks or grants, to encourage SMEs to invest in privacy-enhancing technologies and staff training programs (Mitra, 2023).

Industry self-regulation should also be promoted, with businesses forming alliances to establish best practices for data protection. Certification programs, akin to ISO standards for data privacy, could incentivize compliance by serving as a mark of trustworthiness for consumers.

7.4 Balancing Innovation and Privacy

Overly rigid regulations can stifle innovation, especially in sectors reliant on data-driven technologies like artificial intelligence and targeted advertising. To address this, the government should establish **regulatory sandboxes**, where businesses can test new data processing techniques under controlled conditions, ensuring both innovation and compliance (Shah & Patel, 2023).

Encouraging privacy-by-design frameworks, where data protection is integrated into the development of products and services from the outset, can further support this balance. This approach aligns with global trends and enhances consumer trust without compromising business competitiveness (Tucker, 2014).

7.5 International Collaboration

Given the cross-border nature of data flows, aligning India's data protection framework with global standards like the GDPR and CCPA is imperative. Such alignment would not only facilitate international trade but also enhance consumer confidence in Indian businesses operating globally (Greenleaf, 2022).

India should actively participate in international privacy forums and collaborate on multilateral initiatives to address common challenges like cybercrime, algorithmic bias,

and cross-border data sharing. These efforts could help India position itself as a leader in the global data protection landscape (Nair, 2022).

8. Conclusion

8.1 Summary of Findings

This study has critically examined the intersection of targeted advertising, privacy, and consumer protection under the **Digital Personal Data Protection (DPDP) Act, 2023**. The empirical analysis reveals significant gaps in consumer awareness, with 42% of respondents unaware of their rights under the Act. Business compliance with consent requirements remains inconsistent, while trust in regulatory mechanisms is moderate at best. The study also highlights the duality of targeted advertising, wherein its benefits, such as personalized consumer experiences, are counterbalanced by concerns over privacy invasions and data misuse.

The DPDP Act introduces robust mechanisms for transparency and accountability, aligning with global frameworks such as the **General Data Protection Regulation (GDPR)** and the **California Consumer Privacy Act (CCPA)**. However, challenges persist in the form of regulatory loopholes, enforcement limitations, and business hesitancy to adopt privacy-first practices.

8.2 Implications for Policymakers

Policymakers must prioritize public awareness campaigns to bridge the knowledge gap and empower consumers to exercise their rights effectively. Strengthening the autonomy and capacity of the **Data Protection Board of India (DPBI)** is essential to ensure proactive enforcement. The introduction of regulatory sandboxes could facilitate innovation while maintaining compliance, particularly for startups and SMEs. Policymakers should also address concerns over government exemptions under Section 18, ensuring the Act's credibility as a consumer-centric framework.

8.3 Implications for Businesses

For businesses, the findings underscore the need to adopt privacy-by-design frameworks that integrate data protection into the core of their operations. Simplified consent mechanisms and transparent privacy policies can help rebuild consumer trust. Businesses must also invest in compliance infrastructure, including data audits and staff training, to align with the DPDP Act's provisions. Striking a balance between personalization and privacy will be critical to maintaining competitiveness in the digital economy.

8.4 Future Directions for Research

While this study has provided a comprehensive analysis, several areas warrant further exploration. Future research could examine the long-term impact of the DPDP Act on consumer trust and business practices. Comparative studies across jurisdictions implementing GDPR and CCPA-like frameworks could yield insights into best practices for enforcement. Additionally, empirical research on algorithmic bias in targeted advertising and its socio-economic implications would contribute to a more nuanced understanding of privacy challenges.

8.5 Final Reflection

The DPDP Act represents a significant step toward safeguarding privacy in India's rapidly digitizing economy. However, its success depends on a collaborative effort among policymakers, businesses, and consumers to address implementation challenges and ensure that technological innovation does not come at the expense of fundamental privacy rights. By fostering a culture of transparency, accountability, and ethical data practices, India can position itself as a global leader in data protection and responsible digital innovation.

References

1. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442
2. Gupta, R. (2023). Data privacy challenges in India's digital economy. *Indian Journal of Law and Technology, 19*(3), 45–62. https://www.ijlt.in/articles/dataprivacy2023
3. Greenleaf, G. (2022). Global data privacy laws 2022: A year of convergence. *Privacy Laws & Business International Report, 176*, 1–7. https://www.privacylaws.com/reports
4. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in
5. Nair, V. (2022). Emerging threats to privacy in India's digital landscape. *Economic & Political Weekly, 57*(9), 45–50. https://www.epw.in
6. Shah, S., & Patel, D. (2023). Ethical implications of targeted advertising in India. *Journal of Business Ethics, 178*(1), 123–145. https://doi.org/10.1007/s10551-023-04932-y
7. Supreme Court Observer. (2017). *Case Summary: Justice K. S. Puttaswamy (Retd.) vs. Union of India, 2017*. https://www.scobserver.in/cases/privacy-verdict-puttaswamy
8. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442
9. Chen, Y., Wang, Q., & Li, H. (2021). Artificial intelligence in advertising: Mechanisms, applications, and ethical challenges. *Journal of Marketing Science, 30*(3), 456–475. https://doi.org/10.1177/10565135203003

10. Goldfarb, A., & Tucker, C. (2011). Privacy regulation and online advertising. *Management Science, 57*(1), 57–71. https://doi.org/10.1287/mnsc.1100.1246
11. Kaplan, A. M., & Haenlein, M. (2019). Social media analytics: A powerful tool for targeted advertising. *Business Horizons, 62*(2), 179–189. https://doi.org/10.1016/j.bushor.2019.01.007
12. Mehta, R., Saxena, A., & Saini, S. (2020). Programmatic advertising: Challenges and opportunities. *Digital Advertising Quarterly, 14*(4), 36–48. https://digitaladvertisingquarterly.com
13. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in
14. Shields, M., & Pasternack, S. (2022). The rise of cookies: Tracking users in the digital age. *Journal of Internet Law, 26*(2), 32–45. https://www.journalofinternetlaw.com
15. Tucker, C. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. https://doi.org/10.1509/jmr.10.0357
16. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442
17. Chen, Y., Wang, Q., & Li, H. (2021). Artificial intelligence in advertising: Mechanisms, applications, and ethical challenges. *Journal of Marketing Science, 30*(3), 456–475. https://doi.org/10.1177/10565135203003
18. European Union. (2016). *General Data Protection Regulation (GDPR)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
19. Greenleaf, G. (2022). Global data privacy laws 2022: A year of convergence. *Privacy Laws & Business International Report, 176*, 1–7. https://www.privacylaws.com/reports
20. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in
21. Shah, S., & Patel, D. (2023). Ethical implications of targeted advertising in India. *Journal of Business Ethics, 178*(1), 123–145. https://doi.org/10.1007/s10551-023-04932-y
22. Shields, M., & Pasternack, S. (2022). The rise of cookies: Tracking users in the digital age. *Journal of Internet Law, 26*(2), 32–45. https://www.journalofinternetlaw.com
23. Supreme Court Observer. (2017). *Case Summary: Justice K. S. Puttaswamy (Retd.) vs. Union of India, 2017*. https://www.scobserver.in/cases/privacy-verdict-puttaswamy
24. Tucker, C. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. https://doi.org/10.1509/jmr.10.0357
25. European Union. (2016). *General Data Protection Regulation (GDPR)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
26. Greenleaf, G. (2022). Global data privacy laws 2022: A year of convergence. *Privacy Laws & Business International Report, 176*, 1–7. https://www.privacylaws.com/reports

27. Gupta, R. (2023). Data privacy challenges in India's digital economy. *Indian Journal of Law and Technology, 19*(3), 45–62. https://www.ijlt.in/articles/dataprivacy2023
28. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in
29. Nair, V. (2022). Emerging threats to privacy in India's digital landscape. *Economic & Political Weekly, 57*(9), 45–50. https://www.epw.in
30. Gupta, R. (2023). Data privacy challenges in India's digital economy. *Indian Journal of Law and Technology, 19*(3), 45–62. https://www.ijlt.in/articles/dataprivacy2023
31. Greenleaf, G. (2022). Global data privacy laws 2022: A year of convergence. *Privacy Laws & Business International Report, 176*, 1–7. https://www.privacylaws.com/reports
32. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in
33. Mitra, S. (2023). Challenges in implementing privacy laws for SMEs in India. *Economic & Political Weekly, 58*(4), 15–20. https://www.epw.in
34. Nair, V. (2022). Emerging threats to privacy in India's digital landscape. *Economic & Political Weekly, 57*(9), 45–50. https://www.epw.in
35. Shah, S., & Patel, D. (2023). Ethical implications of targeted advertising in India. *Journal of Business Ethics, 178*(1), 123–145. https://doi.org/10.1007/s10551-023-04932-y
36. Tucker, C. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. https://doi.org/10.1509/jmr.10.0357
37. Gupta, R. (2023). Data privacy challenges in India's digital economy. *Indian Journal of Law and Technology, 19*(3), 45–62. https://www.ijlt.in/articles/dataprivacy2023
38. Greenleaf, G. (2022). Global data privacy laws 2022: A year of convergence. *Privacy Laws & Business International Report, 176*, 1–7. https://www.privacylaws.com/reports
39. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in
40. Mitra, S. (2023). Challenges in implementing privacy laws for SMEs in India. *Economic & Political Weekly, 58*(4), 15–20. https://www.epw.in
41. Nair, V. (2022). Emerging threats to privacy in India's digital landscape. *Economic & Political Weekly, 57*(9), 45–50. https://www.epw.in
42. Shah, S., & Patel, D. (2023). Ethical implications of targeted advertising in India. *Journal of Business Ethics, 178*(1), 123–145. https://doi.org/10.1007/s10551-023-04932-y
43. Tucker, C. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. https://doi.org/10.1509/jmr.10.0357

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.