January 2026 www.cercindia.org

GRAHAK SATHI

Data Privacy & Consumer Rights

Law Students Perspectives on Consumer Rights

International Data Privacy Day

28 January 2026

CONSUMER EDUCATION AND RESEARCH CENTRE
AHMEDABAD

Email : cerc@cercindia.org, grahaksathi@cercindia.org

HELPLINE NO. 1800 233 0332

International Data Privacy Day is observed on 28 January to raise awareness about the importance of protecting personal data and respecting the privacy rights of individuals. The day focuses on increasing public understanding of how personal information is collected, used, shared, and the risks that arise from misuse or inadequate safeguards in an increasingly digital world.

Data privacy is also highly relevant from a consumer protection perspective, particularly in digital marketplaces where consumer data is routinely collected for transactions, profiling, advertising, and service delivery. Weak data protection practices can expose consumers to misuse of information, unfair practices, and loss of trust.

As part of our youth engagement initiatives, we invited our legal interns from law schools to examine data privacy issues through the lens of law and consumer protection. Their papers analyse key concerns such as consent, personal data protection, regulatory frameworks, and the challenges posed by emerging digital business models.

We are pleased to present these essays, which offer informed perspectives and practical insights on data privacy and highlight the need for greater awareness and stronger safeguards in the digital ecosystem.

International Data Privacy Day
28 January 2026

The thoughts of the students do not necessarily represent the views of CERC

Index

Data Privacy in India: A Personal Reflection

-By Aarnav Gandhi
BA LLB, BITS Law School

I'm increasingly worried about how our personal data is handled today. Almost everything we do - banking, shopping, healthcare and education - requires us to share sensitive information like names, addresses, financial details, Aadhaar numbers and even health records. Massive databases, whether government-run or private, store this information, often without us knowing how securely it is kept. When reports emerged that the personal data of 815 million Indians, including Aadhaar and passport details, was allegedly offered for sale online, it sent a chill down my spine. It feels like our privacy is always under threat.

What makes this worse is how little people know about their rights. A PwC survey revealed that only 16% of Indians are aware of the new data protection law and more than half don't even know their basic data rights. If people don't know what protections they're entitled to, how can they question misuse or demand accountability? This lack of awareness allows companies to collect and process data with minimal resistance, often hidden behind long, unread consent forms.

Key Concerns around Data Privacy in India

One major concern is massive data collection. From telecom companies to banks to government schemes, almost every service asks for personal information. We rarely know who stores this data, for how long or how safely. Aadhaar-related leaks have only reinforced the fear that once data is shared, we lose control over it.

Another issue is low awareness and passive consent. Many people don't realise they can withdraw consent after giving it. Studies show that nearly 69% of consumers didn't know they could revoke consent. Most of us click ''I agree'' without reading, unknowingly giving away more information than necessary.

Then there is over-sharing by apps and companies. Many apps demand access to location, contacts or storage even when it's not essential to their function. Users are rarely told how this data is used or shared.

Common Types of Data Breaches

Understanding how breaches occur helps explain why concerns are so widespread.

- Hacker attacks are common. For example, data from 180 million Domino's India pizza orders including names, phone numbers and even credit card details was leaked. Similar breaches have hit e-commerce and social media platforms.
- Insider leaks are equally dangerous. In one reported case, a woman in Noida lost ₹1.4 lakh after a scammer armed with her PAN details and transaction history, posed as a bank official. In many cases, insiders sell customer data to fraud networks.
- Phishing and social engineering exploit trust. Fraudsters often already have partial information from earlier leaks, making their scams more convincing and destructive.
- Poorly secured databases also cause damage. In 2021, COVID-19 test results of thousands of Indians were found indexed on Google not because of hacking, but due to careless storage practices.

Impact on Ordinary Consumers

The consequences for individuals are severe. Financial losses can wipe out savings or result in fraudulent loans taken in someone's name. Constant spam calls and messages are daily reminders that our data has been misused. Beyond money, there is stress, anxiety and loss of trust especially when sensitive health or biometric data is involved. Over time, this distrust discourages people from using digital services, slowing India's digital growth.

Gaps in India's Data Protection Framework

Although India enacted a comprehensive data protection law only recently, gaps remain. For years, the country relied on the outdated IT Act, allowing companies to hide or delay disclosure of breaches. Even now, enforcement is a concern. The Data Protection Board is government-appointed, raising questions about independence. Unlike EU laws, there is no strict timeline requiring companies to inform users of breaches**.**

Critics also highlight broad government exemptions for reasons like "public order," which may leave citizen data vulnerable. These loopholes reduce the law's effectiveness.

Basic Data Rights everyone should know

Despite these challenges, citizens do have important rights:

- The right to know what data a company holds about you and how it is shared
- The right to correct or delete inaccurate or unnecessary data
- The right to give and withdraw consent at any time

- The right to refuse excessive data collection
- The right to complain and seek redress if data is misused

Conclusion

Our personal data is a valuable asset. Protecting it requires not just laws, but awareness, accountability, and vigilance. By understanding our rights, questioning unnecessary data demands and speaking up when things go wrong, ordinary citizens can drive change. A safer digital future is possible but only if we treat privacy as something worth defending.

Data Privacy and Consumer Rights (Privacy as Fundamental Consumer Right)

-By Atulpranav S R
B.COM. LLB, O.P. Jindal University

In my view, in the digital age, data has emerged as one of the most valuable commodities, transforming how businesses operate and consumers interact with services. However, this data-driven economy has raised critical concerns about privacy and consumer protection. Data privacy and consumer rights have become inextricably linked, as personal information forms the foundation of modern consumer transactions. The intersection of these two domains presents unique challenges and necessitates robust legal frameworks to protect individuals from exploitation and ensure fair market practices. In India, this linkage was constitutionally affirmed in Justice K.S. Puttaswamy v. Union of India, where the Supreme Court recognized privacy as a fundamental right intrinsic to individual autonomy, thereby laying the foundation for its treatment as a core consumer protection concern in the digital economy.

The Digital Consumer Landscape

I can confidently say that contemporary consumers engage with digital platforms daily, often unknowingly surrendering vast amounts of personal data in exchange for services. From social media interactions to e-commerce transactions, every digital footprint creates a data trail that companies collect, analyze, and monetize. This asymmetric relationship between data collectors and consumers has created a power imbalance where individuals have limited control over their information. Consumers routinely consent to extensive data collection while using essential services such as e-commerce platforms, digital payment applications, and social media, often without a genuine understanding of how their data is processed or shared. The opacity of data collection practices, combined with complex privacy policies written in legal jargon, leaves consumers vulnerable to exploitation and commercial profiling. Moreover, the global nature of digital commerce means that data flows across jurisdictions, complicating regulatory oversight and enforcement.

Privacy as a Fundamental Consumer Right

We can see that data privacy has evolved from a mere preference to a legally enforceable consumer right. In India, the Supreme Court in Justice K.S. Puttaswamy v. Union of India affirmed informational privacy as an essential facet of personal liberty, recognizing an individual's right to control the dissemination of personal data. This recognition is crucial in the consumer context, where personal information forms the basis of modern commercial transactions.

The right to privacy encompasses informational self- determination, the ability of individuals to control how their personal data is collected, processed, and shared. This right is essential for consumer autonomy and dignity in the digital marketplace. When consumers lack privacy protections, they face risks including identity theft, financial fraud, discriminatory pricing, and unauthorized surveillance. Furthermore, privacy violations can lead to psychological harm and erosion of trust in digital services. Recognizing privacy as a consumer right acknowledges that individuals should not be forced to choose between accessing essential services and protecting their personal information.

Regulatory Frameworks and Their Impact

Several jurisdictions worldwide have responded to data privacy concerns with comprehensive legislation. In 2019, the General Data Protection Regulation (GDPR) established a gold standard for data protection, granting consumers rights including access, rectification, erasure, and portability of their data by the European Union. In India, the Digital Personal Data Protection Act, 2023, empowers consumers, as data principals, with rights relating to consent, correction, and grievance redressal, while imposing corresponding duties on data fiduciaries to process data lawfully, transparently, and for limited purposes. These frameworks require transparent privacy notices, meaningful consent mechanisms, and accountability measures. However, implementation challenges persist, including enforcement capacity, technical compliance burdens on businesses, and the need for consumer awareness. The effectiveness of these regulations depends not only on their provisions but also on robust enforcement mechanisms and accessible redressal systems.

Challenges and Future Directions

We can also see that despite legislative progress, significant challenges remain in protecting consumer privacy rights. The rapid evolution of technology, including artificial intelligence and machine learning, creates new privacy risks that existing laws may not adequately address. Cross-border data transfers complicate jurisdictional enforcement, while small businesses struggle with compliance costs.

Additionally, the notice-and-consent model has proven insufficient, as consumers rarely read lengthy privacy policies and lack genuine choice when services are essential. Future approaches must emphasize privacy-by-design principles, strengthen enforcement mechanisms, promote data

minimization, and develop international cooperation frameworks. Consumer education and empowerment are equally crucial to ensure individuals can effectively exercise their rights.

Conclusion

I would like to conclude by stating that data privacy and consumer rights are inseparable in the digital economy. As personal information becomes increasingly valuable, protecting consumer privacy is not merely a regulatory obligation but a prerequisite for fair and trustworthy markets. Effective protection requires a multi-stakeholder approach involving comprehensive legislation, corporate accountability, technological innovation, and consumer empowerment. Without meaningful enforcement and corporate accountability, privacy protections risk remaining symbolic, making it imperative that consumer protection in the digital age treats data privacy not

Data Privacy and Consumer Rights

-By Hiteshree Naidu
BA LLB, Marwadi University

Data, Dignity, and the Young Consumer: Re-examining Privacy and Power in India's Digital Marketplace

India's youth stands at the intersection of unprecedented digital access and unprecedented data exposure. Education, employment, financial inclusion, and social participation increasingly depend on digital platforms that function through constant data collection. In this ecosystem, young individuals are not merely citizens or users; they are consumers in a data driven marketplace. From this vantage point, data privacy is not an abstract constitutional concern but a question of consumer dignity, fairness, and control. While Indian law has begun responding to this challenge, the protection it offers remains conceptually incomplete and structurally weak.

Diagnosing the Shift: From Consumer to Data Resource

Traditional consumer protection law in India was premised on a clear exchange: money for goods or services. Harm was tangible and traceable. In the digital economy, this model has fractured. Young consumers now pay not only with money but with personal data often without clarity on the scope, duration, or consequences of this exchange. Data is no longer ancillary to consumption it is central to it.

This shift creates a unique form of consumer vulnerability. Data related harm is diffuse and cumulative. A single instance of data collection may appear harmless, but continuous aggregation enables profiling, behavioural prediction, and economic manipulation. Indian consumer law has yet to fully internalise this reality. The absence of a framework that recognises data exploitation as consumer harm leaves young individuals exposed to practices that are neither transparent nor contestable.

Legislative Response Progress with Structural Limitations

India's data privacy framework deserves recognition for acknowledging personal data as an interest requiring regulation. The imposition of duties on entities handling data reflects a growing awareness that digital markets require accountability. For the youth, this legislative acknowledgment is significant it challenges the assumption that participation in digital life necessitates unconditional exposure.

However, the framework's internal logic reveals a critical limitation. The law is constructed around individual consent, assuming that consumers can meaningfully evaluate and control data practices. For young consumers, this assumption is unrealistic. Digital platforms essential for everyday life online classrooms, employment portals, digital wallets offer no meaningful negotiation. Acceptance of expansive data terms is the price of entry. When access is conditional, consent loses its voluntary character.

By prioritising consent over conduct, the law places responsibility on individuals rather than on market actors best positioned to prevent harm. This inversion weakens consumer protection and allows systemic exploitation to persist under formal compliance.

Power without Visibility: The Algorithmic Gap

One of the most serious gaps in Indian consumer law is its inability to address algorithmic power. Digital platforms do not merely host transactions; they actively shape consumer behaviour. Through data analytics, platforms determine visibility, recommend products, influence attention, and personalise prices. For young consumers, this means that choices are filtered before they are consciously made.

Despite its impact, this form of influence escapes traditional legal scrutiny. There is no misrepresentation, no defective service only invisible steering. Indian consumer protection law does not clearly categorise algorithmic nudging or behavioural manipulation as unfair trade practices. As a result, some of the most intrusive forms of exploitation remain legally unarticulated and therefore unregulated.

Enforcement and Access: Rights without Reach

Even where legal protections exist, their enforcement remains inaccessible. Young consumers face a fragmented remedial landscape. Consumer forums lack explicit mandates to address data centric grievances, while specialised regulatory bodies often require technical knowledge and procedural familiarity. This complexity discourages engagement and reinforces a sense of inevitability around data misuse.

The imbalance is stark. On one side are young individuals with limited resources and digital fatigue; on the other are corporations equipped with proprietary technologies, legal teams, and

economic leverage. A system that relies on individual enforcement in such conditions effectively immunises structural misconduct.

Comparative Lessons: From Individual Blame to Structural Accountability

Comparative legal developments demonstrate a gradual shift away from individual- centric models. Several jurisdictions now treat data exploitation as a collective consumer concern. They regulate manipulative digital designs, demand algorithmic transparency, and enable collective redress for systemic violations. These approaches acknowledge that digital harms are rarely isolated or accidental they are embedded in business models.

India's cautious approach is understandable given its scale and socio-economic diversity. However, caution must not result in regulatory inertia. Selective adaptation particularly in recognising collective harm and regulating exploitative design can strengthen consumer protection without undermining innovation.

Reconstructing Consumer Protection for the Digital Youth

From a youth-centric perspective, reform must begin with a conceptual shift. Data privacy should be embedded within consumer protection as a matter of market fairness. Certain data practices excessive retention, behavioural profiling of young users, algorithmic price discrimination should be restricted irrespective of consent. Consumer forums must be empowered to address data related harms, including non-economic injuries such as loss of autonomy and dignity.

Equally vital is digital literacy. Awareness is not a luxury when digital participation is compulsory. Simplified disclosures, standardised consent mechanisms, and public education initiatives must be treated as enforceable obligations.

Conclusion

India's youth does not seek insulation from technology but accountability within it. A legal framework that acknowledges data risks yet defers to consent fails to confront the realities of digital power. Until consumer protection law evolves to address data exploitation as a structural market issue, young consumers will remain visible participants but invisible rights-holders. The future of digital India depends on whether law chooses to protect dignity alongside data.

Data Privacy and Consumer Rights: Bridging the Gap in India's Digital Age

-By Jahan Jethani
BBA LLB, O.P. Jindal University

The digital revolution has transformed how businesses collect, process, and monetize consumer data, making data privacy a fundamental consumer right rather than a mere privilege. As India emerges as one of the world's largest digital economies with over 700 million internet users, the intersection of data privacy and consumer protection has become increasingly critical. While India has taken significant strides with the Digital Personal Data Protection Act of 2023, a comparative analysis with global frameworks reveals substantial gaps in consumer awareness, enforcement mechanisms, and regulatory oversight that demand urgent attention. The stark disparity between India's preparedness and that of developed economies underscores the need for comprehensive reforms to protect consumer rights in the digital age.

The Global Context: Consumer Awareness and Compliance

The European Union's General Data Protection Regulation, implemented in 2018, has set a global benchmark for data privacy legislation. By 2024, EU nations reported over 200,000 data breach notifications collectively, with the Netherlands alone recording 33,471 breaches representing a 65% increase from the previous year. Despite these challenges, consumer awareness in Europe remains remarkably high, with approximately 90% of consumers stating they would not purchase from companies that fail to protect their personal data. The GDPR has imposed cumulative fines exceeding €5.88 billion since inception, demonstrating robust enforcement that holds organizations accountable. Similarly, California's Consumer Privacy Act has shown promising results, with 60% of Californian consumers now aware of their rights and approximately 75% of businesses correcting compliance issues within 30 days of notification. In stark contrast, India presents a troubling picture. A comprehensive PwC survey revealed that only 16% of Indian consumers understand the Digital Personal Data Protection Act, while 56% remain unaware of their rights related to personal data.

This awareness gap is compounded by the fact that 69% of Indian consumers believe their data may not be safe with companies, and only 24% of Indian organizations feel prepared for privacy challenges posed by emerging technologies.

Critical Loopholes in Indian Consumer Protection Framework

The current Indian consumer protection landscape suffers from several critical loopholes that undermine consumer rights. The DPDPA contains broad exemptions allowing government agencies to demand user data without informing individuals, effectively undermining the 2017 Supreme Court judgment recognizing privacy as a fundamental right. Unlike the EU's independent data protection authorities, India has established a Data Protection Board with only four members appointed by the government to oversee privacy for 1.4 billion people, creating severe capacity constraints and questionable independence. The Act applies only to digital personal data, leaving physical records completely unprotected and failing to address comprehensive consumer protection across formats. Retention loopholes embedded in other laws regarding payments, taxation, and e-commerce mean companies must store data for extended periods, significantly weakening the right to erasure even after consumers discontinue services.

The Act fails to adequately categorize sensitive information, potentially leaving critical health, genetic, and biometric data insufficiently protected unlike the GDPR's robust framework. Children's privacy provisions requiring strict age verification and parental consent are deeply flawed in the Indian context where many children are primary digital users in their homes. The absence of Standard Contractual Clauses for international data transfers creates uncertainty and requires extensive negotiations, leading to inconsistent protection standards.

Pathways to Improvement

To address these deficiencies and strengthen consumer rights, India must undertake comprehensive reforms across multiple dimensions. The Data Protection Board must be transformed into an autonomous authority with independent rule-making power, adequately staffed with subject matter experts and granted operational independence from government interference. Organizations should be legally required to invest in consumer rights awareness programs, as currently only 42% of Indian organizations see DPDP Act compliance as an opportunity to build consumer trust. Retention requirements across sectoral laws must be harmonized to align with data minimization principles, ensuring the DPDP Act takes precedence over conflicting obligations unless there is compelling legal justification. India should establish clear breach notification timelines, standardized templates, and meaningful penalties for delayed notifications, similar to the GDPR's 72-hour rule.

The government must work with industry to develop technical standards for consent management, age verification, and data security that are contextually appropriate for India's digital literacy landscape. Sector- specific implementation guidelines would provide clarity while ensuring comprehensive protection, particularly for healthcare, financial services, and education sectors. Strengthening provisions for consumer class action lawsuits would allow collective redress for widespread privacy violations, creating meaningful deterrents against non-compliance.

Conclusion

India stands at a critical juncture in its data privacy journey. While the DPDPA represents a significant legislative milestone, its effectiveness will ultimately be determined by implementation rigor, enforcement credibility, and genuine consumer empowerment. The path forward requires coordinated action: government must demonstrate commitment to independent oversight and transparent enforcement; businesses must view privacy compliance as a competitive advantage rather than a regulatory burden; and civil society must actively engage in awareness campaigns and advocacy efforts. Only through such collaborative efforts can India build a data protection regime that genuinely safeguards consumer rights while fostering innovation and economic growth in the digital economy, bridging the gap between legislative intent and practical implementation to ensure that India's digital citizens receive the protection they deserve.

The Illusion of Consent: Data Privacy as a Consumer Right in India

-By Shivansh Singh
BA LLB, O.P. Jindal University

In India, data privacy is not just a matter of technology, governance, or national security; it is also a matter of consumer rights. Personal information is no longer shared voluntarily or infrequently by the average Indian consumer; rather, it is constantly given up in order to engage in daily activities. Personal information must be disclosed in order to open a bank account, access welfare programs, use UPI payments, enroll in online courses, place food orders, or apply for jobs. Data transactions are opaque and non-negotiable, in contrast to traditional consumer transactions where the consumer can evaluate price, quality, and alternatives. This puts data privacy squarely within the framework of consumer protection and makes Indian consumers particularly vulnerable.

India's data protection framework is an official recognition of the need for legal protections for personal data. It establishes requirements for organizations gathering data, consent-based processing, and grievance redressal procedures. However, consent in India is mostly illusory from the standpoint of the consumer.

The majority of digital services follow a "take-it-or-leave-it" business model, meaning that customers who refuse to give their consent are essentially shut out of necessary services. Consent becomes structurally coerced in a nation where digital access is increasingly linked to healthcare, financial inclusion, and welfare delivery. Consumer autonomy is based on the ideal of free and informed consent, which stands in stark contrast to this. Because of this, Indian consumers frequently view data protection laws as formal promises divorced from everyday life rather than as empowering tools.

This disparity is highlighted when compared to the United Kingdom. Individuals are treated as rights-holders under the UK's rights-based data protection regime, and their consent must be meaningful and revocable. With the help of an active and visible regulator, consumers have clear

rights like access, erasure, and objection. Although consent fatigue and excessive cookie banners are problems for UK consumers as well, they typically operate in an environment where enforcement actions are public, penalties are real, and awareness of privacy rights is relatively high. In India, on the other hand, enforcement is still mostly reactive, consumer awareness is low, and regulatory capacity is overburdened. As a result, rather than being disputed, privacy violations are normalized.

The United States offers a cautionary comparison for India. U.S. data protection is fragmented and market-driven, treating privacy primarily as a matter of consumer choice and contract. Companies collect extensive behavioural data and shift the burden onto consumers to opt out. India's platform economy increasingly mirrors this approach, particularly in e-commerce, fintech, and gig work, where data extraction is aggressive and continuous.

However, unlike the U.S., Indian consumers lack strong collective remedies such as class actions, punitive damages, or well-funded consumer advocacy institutions. This creates a dangerous imbalance: Indian companies adopt U.S.-style data practices without the countervailing consumer power that exists, at least in limited form, in the American system.

A different model is required—the Japanese one, based on trust, measured restraint, and corporate responsibility. Japanese law relies on purpose limitation and proportionality principles, with corporate culture demonstrating conservative data collection out of robust reputation-driven motives. Japanese consumers live in a community where irresponsible personal data use is stigmatized both in society and in company culture. Transferability to Indian reality is a problem. Indeed, the Indian digital economy is highly competitive with price consciousness, with major platforms having negligible reputational risk for excessive personal data collection. Indian consumers cannot very well bank on corporate restraint for a resource that is a vital commercial tool.

The Switzerland model throws more light on flaws present in the India model. The law regarding data protection in Switzerland sets intense restrictions upon data collection, has imperative norms of necessity and proportionality, and ensures effective recourse against abuse. More specifically, state intervention into personal data has intense supervision. The India model has widespread immunity for government departments, which erodes citizen confidence into the entire framework of data protection regulation overall. If any citizen understands government intervention into their data with little transparency or state regulation, it casts doubt upon trust for data security against corporations.

But in all these cases, the most prominent loophole that Indian consumers are left vulnerable to is structural. Consent is often forced, privacy policies are impenetrable, and data sharing is a non-transparent afterthought. As soon as the data is collected, consumers no longer have agency over how it is retained, how it is shared, or how it is sold. The work of data brokers, analytics vendors, and advertisers is carried out out-of-sight for the consumer. Algorithmic accountability is a

problem on top of this problem because it is left impossible for consumers to contest their ranking decisions on issues such as lending, hiring, or pricing.

Grievances can theoretically be addressed through grievance mechanisms. They are slow, cumbersome, and intimidating for individual consumers. It is a historic step for data privacy to become a legal right in India, but it has yet to lead to adequate protection of consumer rights in the country. On a comparison of Indian laws and those of the UK, USA, Japan, and Switzerland, it is found that it is not enough to have strong rights if it is weak in implementation, broad government exemption, opaque algorithms, and limited remedies.

About CERC

Consumer Rights, Protection and Justice for consumers have been the focus of Consumer Education and Research Centre (CERC) since its inception in 1978. CERC is India's only Consumer Rights Organisation that provides 360° services to the consumer in terms of Education, Empowerment and Protection.

A broad range of activities are undertaken in the organization – grievance redressal through mediation and litigation, consumer education and awareness building through various publications and outreach activities, testing and analysis of consumer products in our in-house product testing laboratories, advocacy for laws and regulations that better protect consumers, as well as a number of projects executed in various areas pertinent to consumer protection and empowerment. Promoting environmental awareness, energy conservation and sustainable consumption are also major activity areas in CERC.

Grahak Sathi - your weekly e-magazine is available free in English, Hindi, Gujarati, Malayalam, Marathi, Tamil and Bengali. If you want to receive a free copy, write to us at grahaksathi@cercindia.org.

CERC Team

CEO
Anindita Mehta

Associate Editors
Anusha Iyer, Rashmi Goyal

Staff Writer
Tithi Bhandari

Consumer Education Research Centre

'Grahak Suraksha Kendra'
8th floor, Sakar 2,
Next to Ellisbridge Police Station,
Ashram Road, Ahmedabad - 380006