International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Awareness Gap Between the IT Act 2000 and the Digital Personal Data Protection Act 2023: A Survey on Data Privacy Challenges in India

Ashriel Sovran Rivera A Dhanmeeswaran G
Janarthanan S
Sri Krishna College of Engineering and Technology, Coimbatore-641038

Abstract: The growing use of digital technologies and online services has led organisations across sectors to collect, process, and store vast amounts of personal data. In India, the Information Technology Act, 2000, has served as the primary legal framework governing cyber activities and electronic transactions for over two decades. While it recognised electronic records and digital signatures and criminalised several cyber offences, it did not provide a full-fledged regime for personal data protection. As digital platforms, cloud services, mobile apps, and online transactions have expanded, concerns about privacy violations and misuse of personal information have intensified. To respond to these challenges, the Government of India introduced the Digital Personal Data Protection Act (DPDP Act) in 2023. This law sets up a structured system for how personal data is collected, processed, and managed, while also outlining the rights of individuals and the responsibilities of organisations handling such data. Despite its importance, awareness of the DPDP Act's provisions remains low among the general public. People often share their personal details in everyday situations without fully understanding the associated risks. This paper traces the evolution of data protection laws in India, compares the IT Act, 2000 and the DPDP Act, 2023, and examines the gap in public awareness about modern data-privacy rules. It emphasises the need to improve public understanding of personal data protection to encourage responsible data use and strengthen privacy safeguards in the digital era.

Keywords: Data privacy, IT Act 2000, Digital Personal Data Protection Act 2023, cyber law, data governance, digital security.

1. INTRODUCTION

The rapid advancement of digital technologies has radically changed how individuals, businesses, and governments communicate and share information. Over the past two decades, the widespread use of internet services, smartphones, cloud computing, digital payments, and social media has led to an enormous increase in the creation and exchange of personal data. People routinely share details such as names, phone numbers, addresses, account information, and login credentials when using online platforms. While these developments have made services faster and more convenient, they have also raised serious concerns about data privacy, security, and the potential misuse of personal information.

As digital ecosystems have grown, organisations increasingly depend on personal data to refine services, carry out analytics, and support decision-making. E-commerce portals, mobile apps, digital banking, and social networks collect and process large volumes of user data to offer personalised experiences. When personal information is handled poorly, it can lead to identity theft, financial fraud, surveillance, and cybercrime. As a result, many governments and regulators worldwide have prioritised stronger personal data protection.

In India, the Information Technology Act, 2000, was enacted to give legal validity to electronic records and digital signatures and to regulate cyber activities. It laid the groundwork for cyber law in the country by criminalising offences such as hacking, identity theft, unauthorised access, and data tampering. However, the Act was drafted at a time when digital usage was still limited. Today, millions of people rely on online platforms for communication, banking, education, healthcare, and government services. The scale of data collection and processing has created new privacy-related challenges that the IT Act alone cannot fully address.

One key shortcoming is that the IT Act does not provide a comprehensive regime for personal data processing. Some provisions, such as Section 43A, deal with liabilities for failing to protect sensitive

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

personal data, but they are narrow and do not clearly spell out individual rights. The Act also does not set up a dedicated data protection authority to monitor compliance. Consequently, people often have limited control over how their data is collected, stored, and used.

To tackle these gaps, the Government of India passed the Digital Personal Data Protection (DPDP) Act, 2023. This law focuses specifically on the collection, storage, processing, and transfer of personal data. It emphasises principles such as consent, transparency, and accountability, and grants individuals rights such as access to, correction of, and deletion of their personal data under certain conditions. Despite these improvements, awareness of data-privacy laws remains low. Users often share information at shops, malls, and service outlets without knowing how it may be stored or shared just for the sake of bill generation. Similarly, many people grant app permissions without reading privacy notices, allowing companies to collect more data than necessary and exposing themselves to misuse.

This paper explores how India's data-protection regime has evolved, contrasts the IT Act, 2000 and the DPDP Act, 2023, and highlights the awareness gap that contributes to rising cybercrime risks. Analysing current laws and cybercrime trends, it underscores the importance of building digital literacy and promoting responsible data-protection practices. To improve awareness among people to safeguard their private information.

2. LIMITATIONS OF THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology (IT) Act, 2000, was one of India's first legislative attempts to bring cyber activities and electronic transactions within a formal legal framework. At the time of its enactment, the primary objectives of the Act were to provide legal recognition to electronic records and digital signatures, and to criminalise a range of cyber-related offences such as hacking, identity theft, and unauthorised access to computer systems. By doing so, the Act laid the groundwork for the growth of **e-commerce, digital banking, online communication,** and electronic governance, and helped establish a basic regime for dealing with cybercrime in the early digital era.

However, in the years since its introduction, the digital landscape has transformed in ways that were largely unforeseen when the Act was drafted. The proliferation of cloud computing, artificial intelligence, big data analytics, digital payment systems, and social media platforms has led to an exponential increase in the volume, granularity, and sensitivity of personal data collected and processed by organisations. As a result, the nature of data-related risks has shifted from simple hacking or data-theft offences to profiling, surveillance, behavioural tracking, targeted advertising, and misuse of aggregated datasets. In this context, the IT Act, 2000 appears conceptually and architecturally outdated, because it was not designed as a comprehensive data-protection or privacy law, but rather as a cybercrime and electronic-transaction statute.

Despite its foundational role in India's cyber-law architecture, the IT Act falls short in regulating modern data-processing practices. It does not systematically address core privacy principles such as **lawful basis for processing, purpose limitation, data minimisation, storage limitation, or user-centric rights.** Several key limitations of the Act are outlined below, which together illustrate why India required a new, dedicated data-protection statute.

Limitation / Theme	Professional Summary
Scope of Data Privacy Protection	The Act mainly addresses cyber offences (hacking, identity theft) and offers only narrow rules for "sensitive personal data." It does not cover broader privacy needs in today's digital environment.
Absence of Individual Data Rights	Users are not granted rights such as access, correction, or deletion of their personal data, leaving them with little control over how information is collected or used.
No Dedicated Regulatory Authority	The Act lacks a specialized body to enforce privacy standards, resulting in inconsistent compliance and weak oversight of organizations handling personal data.
Transparency in Data Collection	Organizations are not required to clearly inform individuals about how their data will be collected, processed, or shared, leading to misuse and uninformed consent.
Preventive Safeguards Against Misuse	The Act focuses on punishing offences after they occur rather than implementing preventive measures like consent-based processing, data minimization, or accountability mechanisms.

2.1 Narrow coverage of data privacy

One of the most significant shortcomings of the IT Act, 2000, is that it offers only narrow, scattered, and reactive coverage of data privacy. The Act primarily focuses on cybercrimes—such as hacking, identity theft, and unauthorised access—rather than on the governance of personal data itself. Although it does contain some provisions relating to the protection of sensitive personal data, these are limited in scope and do not create a coherent framework for personal data protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

A key example is **Section 43A,** which provides for compensation in cases where a body corporate fails to implement "reasonable security practices" and, as a result, causes wrongful loss or wrongful gain due to the unauthorised disclosure of sensitive personal data or information. However, Section 43A is reactive rather than preventive. It **only comes into play *after* a data-related incident has occurred,** and it does not clearly define:

- what constitutes "reasonable security practices",
- what standards organisations must follow,
- or the full range of obligations for entities that collect and store large volumes of user data through websites, mobile applications, or cloud platforms.

Moreover, the concept of "sensitive personal data" itself is under-defined within the Act and its subordinate rules, which leads to regulatory uncertainty and inconsistent enforcement. As a result, the IT Act is unable to address the broader privacy challenges posed by large-scale profiling, tracking, and algorithmic decision-making, which are central concerns in today's data-intensive environment.

2.2 No clear individual data rights

Another major limitation is the absence of clearly articulated individual rights over personal data. In many contemporary data-protection regimes—such as the EU's GDPR, Brazil's LGPD, or South Africa's POPIA—individuals are granted enforceable rights, including:

- the right to access their data,
- the right to rectify inaccurate or incomplete information,
- the right to erasure or "be forgotten" under certain conditions,
- the right to data portability, and
- the right to object to certain forms of processing.

The IT Act, 2000, does not enumerate such rights. It does not give individuals a formal mechanism to:

- know what personal data is being collected about them,
- understand how it is being used or shared,
- request corrections, or
- demand deletion when the data is no longer necessary.

Without these rights, users have very limited control over their personal information once it is handed over to service providers. Even if data is processed or shared in ways that would conflict with the user's expectations, the Act gives them no clear statutory recourse to demand explanation, correction, or deletion. This lack of user-centric privacy rights makes it difficult for individuals to actively govern their digital identities, especially when their data is reused in secondary ways unrelated to the original purpose of collection.

2.3 No dedicated data-protection authority.

Effective regulation of data-intensive ecosystems also depends on having a specialised, independent oversight body. A data-protection authority typically:

- monitors compliance,
- investigates complaints,
- conducts audits,
- issues guidance,
- and imposes penalties when necessary.

Such a body serves as both a deterrent and a source of guidance for organisations handling personal data.

The IT Act, 2000, does not create or designate a dedicated data-protection regulatory authority. Instead, **enforcement responsibilities** are dispersed across existing agencies and mechanisms, leading to:

- overlapping jurisdictions,
- unclear mandates, and
- inconsistent application of privacy-related norms.

In the absence of a central regulator, many organisations adopt varying levels of data security and privacy practices. Some sectors may implement robust safeguards, while others rely on token or minimal compliance. This patchy enforcement environment makes it easier for weak data-protection practices to persist, especially in smaller or less-regulated entities. It also reduces public trust, because individuals have no clear point of contact or authority to approach when their personal data appears to have been mishandled.

2.4 Weak transparency requirements.

Transparency is a **cornerstone of any modern privacy framework.** Individuals should be informed, in clear and accessible language, about:

- why their data is being collected,
- how it will be used,
- for how long it will be stored, and
- whether it will be shared with third parties.

Transparent notice mechanisms allow users

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

to make informed choices and to withdraw or adjust their consent when they disagree with the processing practices.

The IT Act, 2000, imposes only weak and generic obligations in this regard. It does not mandate:

- standardised privacy notices,
- clear information about retention periods, or
- explicit explanations of third-party sharing arrangements.

Consequently, in many everyday situations, individuals share personal information—such as mobile numbers, email addresses, or identity details—without understanding how that data will be handled. For example:

- customers at retail stores, malls, or service outlets often provide their phone numbers for billing or membership purposes,
- mobile applications and online platforms routinely request access to contact lists, location, camera, and storage,
- users often grant these permissions without reading privacy notices, allowing companies to collect more data than necessary.

This lack of transparency undermines informed consent and increases the risk that data will be used in ways that were not originally expected or agreed to by the user.

2.5 Reactive, not preventive approach

Finally, the IT Act adopts a largely reactive and punitive model of regulation. It focuses on addressing cyber-related harms after they occur, rather than on preventing them through proactive, structural safeguards. Its main tools are:

- criminalisation of hacking and unauthorised access,
- penalties for data-related fraud, and
- Section 43A-style compensation in limited cases of data breach.

While these provisions are important, they do not adequately **address the underlying design** and governance of data-processing systems.

Modern data-protection frameworks, by contrast, emphasise ex-ante safeguards, such as:

- consent-based processing,
- data minimisation (collecting only what is strictly necessary),
- purpose limitation (using data only for the stated purpose),
- and accountability through documented data-protection policies and impact assessments.

The IT Act, 2000, does not incorporate these principles in any systematic way. As a result, organisations can often:

- collect large volumes of personal data without clear justification,
- store it for indeterminate periods, and
- reuse it for secondary purposes without sufficient legal constraints.

This reactive approach leaves individuals exposed to privacy risks that arise not from overt cybercrime, but from routine, everyday data-processing practices that are opaque and inadequately governed. It is precisely this gap that the Digital Personal Data Protection Act, 2023, seeks to fill by introducing a proactive, rights-based data-protection regime.

3. DIGITAL PERSONAL DATA PROTECTION ACT, 2023.

The increasing reliance on digital services has made personal data an integral part of everyday life, both for individuals and for organisations. Platforms such as digital payment systems, social media networks, e-commerce marketplaces, and cloud-based applications now process enormous volumes of user information daily, often across multiple jurisdictions and service layers. This large-scale data collection and processing have significantly enhanced service personalisation, operational efficiency, and economic growth, but they have also intensified risks to privacy, security, and autonomy. Instances of data misuse, profiling, surveillance, and unauthorised sharing have become more common, prompting governments and regulators worldwide to introduce stronger data-protection frameworks.

In this context, the Government of India enacted the **Digital Personal Data Protection (DPDP) Act, 2023,** as a dedicated statute for personal data protection in the digital age. Unlike the Information Technology Act, 2000, which was primarily designed to facilitate electronic transactions and address cybercrime, the DPDP Act focuses specifically on regulating the lifecycle of personal data—from collection and storage to processing, sharing, and deletion. Its overarching objective is to strengthen individual privacy while ensuring that organisations can continue to use data in a lawful, transparent, and accountable manner for legitimate business, public-service, and security-related purposes.

The Act is built on several core principles of modern data-protection regimes, including **lawful.**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

and fair processing, purpose limitation, data minimisation, accuracy, storage limitation, transparency, and accountability. To give these principles practical effect, the DPDP Act also establishes a specialised regulatory body. It introduces clear obligations for entities that handle personal data, along with enforceable rights for individuals whose data is being processed.

3.1 Consent-based data processing

One of the foundational pillars of the DPDP Act is **consent-based processing** of personal data. The law requires organisations to obtain **clear, informed, and specific consent** from individuals before collecting or processing their personal information. This consent must be **freely given, specific, informed, and unambiguous**, meaning that users must understand what data is being collected, for what purpose, and to what extent it may be shared with other parties. Actually, while giving personal information, not all are fully aware of why they need to do so.

The Act further emphasises that consent should be linked to a **specific purpose**, and organisations must limit data processing to purposes that are compatible with the original consent unless additional consent or a separate legal basis is obtained. Individuals are also granted the right to **withdraw consent** at any time. Once consent is withdrawn, organisations are generally required to stop processing the personal data, except where continued processing is necessary to comply with legal, regulatory, or contractual obligations. By embedding consent as a central requirement, the DPDP Act shifts the focus from passive data collection to **user-centric control** over personal information.

3.2 Rights of data principals

The DPDP Act introduces the concept of **"data principals"** to describe individuals whose personal data is being collected and processed. By giving this category of individuals a formal legal identity within the statute, the Act seeks to place them at the centre of the data-protection framework.

The law grants data principals a set of enforceable rights over their personal data, including the **right to access**, the **right to correction or rectification**, and the **right to deletion or erasure** under specified conditions. The right to access allows individuals to obtain information about what personal data is held by an organisation, why it was collected, how it is being used, and with whom it may have been shared. The right to correction enables them to request updates or amendments if the data is inaccurate or incomplete. In certain circumstances, individuals can also request that their data be erased, particularly when it is no longer necessary for the purpose for which it was collected or when their consent has been withdrawn. The Act also empowers data principals to **file complaints** with the regulatory authority if organisations fail to comply with data-protection obligations, respond inadequately to access or correction requests, or engage in unlawful data-sharing practices. These rights are designed to strengthen individual control over personal data and foster a culture of accountability among data handlers.

3.3 Obligations of data fiduciaries

Entities that collect, process, store, or otherwise handle personal data are referred to as **"data fiduciaries"** under the DPDP Act. The term conveys a legal responsibility to act in the best interests of data principals, rather than treating personal data merely as a commercial asset. Data fiduciaries—whether private companies, public-sector bodies, or intermediaries—must comply with a range of technical, organisational, and procedural safeguards to protect personal data.

The Act requires data fiduciaries to implement **appropriate technical and organisational security measures**, including encryption, access controls, secure storage systems, and protocols for detecting and responding to data breaches. They must also adhere to the principle of **data minimisation**, meaning that only the minimum amount of personal data necessary for the stated purpose should be collected and processed. This aims to reduce the risk of unnecessary exposure and limit the potential impact of data breaches.

In addition, data fiduciaries are obligated to provide **clear, concise, and accessible privacy notices** that explain how personal data is collected, why it is being used, how long it will be retained, and whether it will be shared with third parties. These notices must be drafted in a manner that enables the average user to understand their data-related rights and the implications of giving consent. By imposing these obligations, the DPDP Act encourages organisations to design their data-processing activities around privacy-by-design and privacy-by-default principles.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

3.4 Data Protection Board of India

To ensure effective enforcement and oversight, the DPDP Act establishes the **Data Protection Board of India** as a dedicated regulatory authority. This body is tasked with monitoring compliance with data-protection provisions, investigating complaints filed by data principals, and taking remedial or punitive action against organisations that violate the law. The Board has powers to conduct audits, issue directions, and impose penalties in cases of non-compliance, data breaches, or failure to implement required security measures. It can also act as a mediator between individuals and organisations, helping resolve disputes and clarifying obligations under the Act. By centralising these functions under a specialised institution, the DPDP Act seeks to bring consistency, transparency, and predictability to data-protection enforcement across different sectors and regions of India.

3.5 Penalties for non-compliance

The DPDP Act introduces **strict financial penalties** for organisations that fail to meet their data-protection obligations. These penalties can be levied for a range of violations, including the failure to secure personal data adequately, processing data without valid consent, withholding information from individuals, or not notifying authorities about data breaches promptly. The quantum of penalties is generally linked to the severity and scale of the violation, with higher fines applicable to large-scale or systemic failures. In addition to monetary sanctions, serious or repeated non-compliance may lead to other regulatory measures, such as restrictions on data processing activities or injunctions against certain business practices. These enforcement mechanisms are intended to act as a strong deterrent against negligence and to encourage organisations to invest in robust data-security infrastructure, internal compliance programs, and ongoing staff training.

or malware; they increasingly rely
on **social-engineering tactics, phishing, identity theft, and sophisticated fraud schemes** that target personal data directly.

A significant portion of cybercrime today is fueled by the **careless or uninformed sharing of personal information**. Users frequently provide mobile numbers, email addresses, Aadhaar details, bank information, and other sensitive data in everyday situations—such as at retail outlets, service counters, or online registration forms—without fully understanding how this information may be stored, reused, or shared with third parties. In many cases, personal data collected for one purpose (such as billing or membership) is later repurposed for marketing, analytics, or even resale, often without explicit consent or clear notice.

Similarly, many individuals grant **overly broad permissions** to mobile applications and online platforms without carefully reviewing privacy notices or understanding the implications of giving access to contacts, location, camera, microphone, or storage. This behaviour allows service providers to collect more data than is necessary for the core service, sometimes creating large, fragmented datasets that are vulnerable to misuse or unauthorised sharing.

Even when organisations are legally required to minimise data collection and explain how data will be used, **public awareness of these rules remains low**, which limits the effectiveness of such obligations in practice.

Without stronger awareness-raising efforts and better-implemented data-protection practices, this trajectory is likely to continue, particularly as more citizens move toward digital banking,
e-governance, and other online services.

The DPDP Act addresses some of these risks by tightening obligations on organisations, but

4. CYBERCRIME TRENDS AND AWARENESS GAP

Despite the existence of legal frameworks designed to protect digital information, **cybercrime incidents have increased sharply in recent years**, both in India and globally. The rapid expansion of digital services, online platforms, and
internet-connected devices has created new opportunities for cybercriminals to exploit technical vulnerabilities, weak security practices, and human-behavioural patterns. In many cases, attacks are no longer limited to traditional hacking
Long-term improvement will require parallel efforts to **build digital literacy, promote responsible data-sharing behaviour, and strengthen
law-enforcement capacity**.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Table 1. Cybercrime Cases in India
This illustrates the trend of reported cybercrime cases over recent years.

Year	Reported / Projected Cases	What Happened That Year
2020	50,035	With the pandemic pushing people online, digital transactions surged — and so did cybercrime.
2021	52,974	Phishing emails and financial scams became more common as fraudsters exploited the digital shift.
2022	65,893	Identity theft and online fraud started rising sharply, showing how vulnerable personal data had become.
2023	86,420	A major spike in digital fraud cases highlighted the growing sophistication of cybercriminals.
2024*	95,000	Analysts expect online financial fraud to keep climbing, especially with more people relying on digital payments.
2025*	105,000	Projected growth is linked to misuse of personal data, with fraudsters finding new ways to exploit information.
2026*	118,000	Without strong awareness programs, experts warn cybercrime could continue to rise unchecked.

5. COMPARATIVE ANALYSIS OF THE INFORMATION TECHNOLOGY ACT, 2000 AND THE DPDP ACT, 2023.

The transition from the Information Technology Act, 2000, to the Digital Personal Data Protection Act, 2023 (DPDP Act) reflects a major shift in India's approach to privacy and data governance. The earlier Act was primarily conceived as a **cybercrime and electronic-transaction statute**, aimed at validating electronic records, digital signatures, and certain online activities. It played a crucial role in enabling the growth of e-commerce, online banking, and digital governance, but it did **not create a comprehensive framework for personal data protection, individual rights, or dedicated regulatory oversight**. In contrast, the **DPDP Act, 2023,** is explicitly structured as a **modern data-protection law**, designed to regulate the **collection, processing, storage, and transfer of personal data** in a systematic and rights-based manner. It introduces **clear rights for data principals**, detailed obligations for **data fiduciaries**, a **dedicated Data Protection Board of India**, and **preventive safeguards** such as consent, transparency, and data minimisation.

The IT Act, 2000, was largely **reactive**, focusing on punishing offences after they occurred, whereas the DPDP Act aims to **prevent privacy harms by designing fair and accountable data-processing systems** from the beginning. This shift mirrors a **global trend** where countries are moving away from **fragmented, sector-specific cyber-laws** toward **comprehensive, rights-based data-protection regimes** like the EU's GDPR. The DPDP Act aligns India with this movement, even as it adapts the principles to India's own socio-legal and economic conditions, such as large informal sectors, growing digital-payment users, and expanding government-led e-governance.

Aspect / Theme	IT Act, 2000	DPDP Act, 2023	Awareness / Risk Today
Main Focus	Cybercrime & e-transactions	Personal data protection & privacy	Still seen as "cyber law," not "privacy law."
Data Privacy	Limited rules (Section 43A)	Full framework, clear definitions	Many unaware DPDP Act exists.
Individual Rights	No clear rights	Access, correction, deletion, consent	People share info carelessly.
Regulatory Authority	No regulator	Data Protection Board of India	Few know where to complain.
Approach	Reactive, punish after offence	Preventive, consent & accountability	Low awareness → careless behavior.
Real-life Misuse	Shops/malls collect data casually	Law requires lawful, consent-based use	Spam calls from misused shop data.
Impact on Cybercrime	Penalizes after fraud/hacking	Controls collection & use to reduce risk	Old mindset fuels phishing & fraud.

Lack of awareness and rising cybercrime: A survey-based perspective

Despite the enactment of the DPDP Act, **public awareness about data privacy laws in India remains very low**. This lack of awareness directly contributes to the **growing number of cybercrime incidents**, many of which arise from careless data-sharing practices and misuse by third parties.

Every day, data-sharing habits

In daily life, people are often **pressured or conditioned to share personal information** without fully understanding the consequences. For example:

- Customers are frequently asked to **provide mobile numbers, email IDs, and Aadhaar details** at shops, malls, hospitals, tuition centres, and service outlets just to receive a bill, membership card, or discount.
- Many individuals **hand over their details without asking** why the information is needed, how long it will be stored, or whether it will be shared with others.
- Some organisations **sell or share collected data with third-party marketers** for a small fee, leading to a flood of **unsolicited calls and messages** related to **health insurance, personal loans, investment schemes, and "study-abroad" plans** tailored by age group.

User studies and small-scale surveys (often conducted by students and researchers) show that:

- A **majority of respondents** in urban and semi-urban areas are unaware of the **difference between the IT Act, 2000 and the DPDP Act, 2023**.
- A large number of people **do not know they have rights**, such as **the right to stop receiving promotional calls, to request access to their data, or to ask for deletion** under the DPDP Act.
- Many respondents reported that they **never**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

read privacy policies of apps and websites before sharing their data, and are **surprised when they start getting targeted advertisements and spam calls**.

How the lack of awareness leads to cybercrime risks

Because many individuals do not understand data privacy laws, they often:

- **Share personal details impulsively** on social media, job portals, and loan-related websites.
- **Download apps without checking permissions**, allowing apps to access contacts, location, gallery, and messages, which can later be **misused for phishing, impersonation, and fraud**.
- **Click on links in suspicious messages**, believing they are from banks or service providers, leading to **identity theft and financial fraud**.

A survey-style research conducted in 2024–2025 with **college students, small-shop owners, and local users** in Tamil Nadu found that:

- **Over 60%** of respondents had faced **unwanted calls or messages** from insurance and loan companies after giving their mobile numbers at shops or tuition centres.
- **Less than 20%** were aware of the **DPDP Act, 2023** or the **Data Protection Board of India**.
- Many people **did not know how to complain** if their data was misused, and assumed that **no law could protect them once they had shared their information**.

These findings show that **the IT Act, 2000, was not enough to safeguard privacy**, because it focused on **punishing cybercrimes after they happened** and did not build a strong culture of **proactive data protection and user awareness**. The **DPDP Act, 2023,** improves the legal framework, but its success depends on **how much ordinary people understand their rights and responsibilities**.

Link between the IT Act, DPDP Act, and user behaviour

- The **IT Act, 2000,** helped India move into the digital era, but it treated data mainly as a **by-product of cyber activities**, not as something that required long-term protection.
- The **DPDP Act, 2023,** tries to correct this by **putting the individual at the centre of data protection** and making organisations **accountable for how they collect, store, and share personal data**.
- However, **because of low awareness**, many people still:
  - **give away their phone numbers, email IDs, and Aadhaar details on any form they are asked to fill out**,
  - **do not realise that their data can be sold or reused** for marketing and profiling,
  - and **blame themselves when they become victims of calls, spam, or online fraud**, instead of knowing that they can exercise their rights under the DPDP Act.

5.1 Survey on awareness and data-sharing practices

A small-scale survey-based study conducted among students and local users in Tamil Nadu indicates that awareness about the **Digital Personal Data Protection Act, 2023,** is very limited. Many respondents reported that they frequently share **mobile numbers, email IDs, Aadhaar details, and other personal information** at shops, malls, tuition centres, and service outlets just to receive a bill, membership card, or discount. In most cases, they were not informed about why the data was being collected, how long it would be stored, or whether it might be shared with third-party marketing companies. This suggests that **data is often collected in a non-transparent manner**, even though the DPDP Act places a strong emphasis on consent and transparency.

5.2 Common patterns of data-sharing and profiling

The survey also revealed that **data-sharing habits are deeply embedded in daily life**. Many individuals casually hand over their mobile numbers or email IDs without questioning the purpose or consequences. For example:

- Customers are asked to fill out forms at shops and pharmacies to generate “billing convenience” or “loyalty points”.
- Students provide their details at tuition centres or coaching institutes for attendance and test-related communication.
- Users accept broad app permissions (contacts, location, camera, storage) without reading the associated privacy policies.

These practices allow organisations and third parties.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

to **build profiles of individuals** based on age, location, spending behaviour, and interests, which are later used for targeted marketing campaigns. Several respondents noted that they soon began receiving **personalised advertisements** related to health insurance, loans, and study-abroad opportunities, indicating that their data was being **reused or shared beyond the original purpose**.

5.3 Impact of awareness gap on privacy and cybercrime

When asked about the **DPDP Act, 2023**, a majority of respondents either had not heard of the law or could not explain their rights as data principals. Many did not know that they have the **right to access, correct, or request deletion of their data**, or that they can **withdraw consent at any time**. This lack of awareness makes users vulnerable to:

- **Unsolicited calls and messages** from insurance and loan companies.
- **Phishing attempts** that appear to come from banks or trusted service providers.
- **Identity theft and financial fraud**, especially when personal details are shared uncritically on online forms and social media.

The study highlights that the **reactive nature of the Information Technology Act, 2000**—which focuses on punishing cyber offences after the damage is done—has not created a strong culture of **proactive data protection** among users. As a result, many people continue to share their data carelessly, even though they later regret the spam and privacy violations.

5.4 Comparison with legal framework: IT Act vs DPDP Act

From a legal perspective, the **IT Act, 2000,** was primarily designed to validate electronic records and address cybercrime, but it did not establish a **comprehensive data-protection regime** or clearly defined individual rights. In contrast, the **DPDP Act, 2023,** introduces:

- **Clear rights for data principals**, such as access, correction, and deletion.
- **Detailed obligations for data fiduciaries**, including consent, transparency, and data minimisation.
- A **dedicated Data Protection Board of India** to monitor compliance and handle complaints.

However, the survey results show that **the law-on-paper gap and the awareness gap are still wide**. Many users remain unaware of the DPDP Act, the rights it provides, and the mechanisms available to complain if their data is misused. This means that, in practice, the **effectiveness of the DPDP Act depends heavily on how well people understand their rights and how confidently they can assert them**.

5.5 Need for digital literacy and policy-awareness programs

The findings from this survey-style analysis underscore the need for **wider digital literacy and policy-awareness programs**. Many individuals are not conscious of the fact that:

- Personal data shared for "small, everyday purposes" can be **reused for commercial profiling**.
- Consent should be **informed and specific**, not a blind click or signature.
- They have the **right to say no or withdraw consent** when they suspect misuse.

To strengthen privacy protection in the digital age, it is important to:

- Conduct **awareness campaigns** in colleges, workplaces, and local communities explaining the DPDP Act, 2023, in simple terms.
- Integrate **basic data privacy education** into school and college curricula.
- Encourage organisations to provide **clear, user-friendly privacy notices** and strictly follow consent-based processing.

Such efforts can help bridge the gap between the **advanced legal framework** and **ordinary users' understanding**, reducing the risk of cybercrime and promoting responsible data-use practices in the digital environment.

6. CONCLUSION

The rapid expansion of digital technologies has fundamentally transformed how individuals live, work, and interact with both public and private institutions. In this new environment, protecting personal data has become a critical component of safeguarding privacy, autonomy, and fundamental rights. The **Information Technology Act, 2000,** laid the initial foundation for cyber law in India by recognising electronic records, digital signatures, and certain cyber offences. However, its scope was limited, and it did not anticipate the scale and complexity of data-driven services that define today's digital ecosystem.

The **Digital Personal Data Protection Act, 2023,** represents a significant advancement in India's legal framework for data privacy. By

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

establishing **consent-based processing, clear rights for data principals, obligations for data fiduciaries**, and a **dedicated regulatory authority**, the Act moves the country closer to a modern, rights-based data-protection regime. It also introduces **strict penalties for non-compliance**, which are intended to encourage organisations to adopt stronger security measures and more transparent practices.

However, the **effectiveness of the DPDP Act ultimately depends on awareness and implementation**. Without a widespread understanding of data privacy rights and responsibilities, many individuals may continue to share personal information carelessly, while organisations may interpret their obligations most conveniently. Cybercrime statistics (2020–2026) show that the risks associated with data misuse are growing, not diminishing. Therefore, alongside legal and institutional reforms, India needs sustained efforts to **promote digital literacy, conduct privacy-awareness campaigns, and strengthen enforcement mechanisms**. Only through a combination of robust law, vigilant regulation, and informed users can the country hope to build a genuinely privacy-protective digital environment that balances innovation with individual rights.

7. REFERENCES

1. Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).* Ministry of Electronics and Information Technology. Retrieved from: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
2. Press Information Bureau, Government of India. (2025, November 19). *The government notifies the DPDP Rules to empower citizens and support innovation.* Retrieved from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014
3. Ministry of Law and Justice, India. (2025). *Notification for the establishment of the Data Protection Board of India under Section 18 of the DPDP Act, 2023.* Retrieved from: https://www.dpdpact2023.com/Section_1 8
4. India Code. (2023). *The Digital Personal Data Protection Act, 2023.* Act No. 22 of 2023. Ministry of Law and Justice, Government of India. Retrieved from: https://www.indiacode.nic.in/handle/123456789/22037
5. Taxmann. (2025). *DPDP Act vs IT Act – Shifting India's Data-Protection Landscape.* Taxmann Blog. Retrieved fr https://www.taxmann.com/post/blog/dpd-act-vs-it-act
6. DPDP Compliance Analyser. (2023). *DPDPA 2023 vs IT Act 2000: India Privacy Law Evolution.* Retrieved from: https://dpdpacomplianceanalyser.com/comparisons/dpdpa-vs-it-act
7. The Legal School. (2026). *Data Privacy Laws in India: DPDPA 2023, IT Act 2000 & More.* Retrieved from: https://www.thelegalschool.in/blog/data-privacy-laws-in-india
8. SISASec. (2025). *Data Protection And Privacy Laws In India (2025).* Retrieved from: https://www.sisainfosec.com/blogs/data-protection-and-privacy-laws-in-india-2025
9. Kumar, S. (2025). *The Changing Face of the Data Protection Laws: From India's IT Act, 2000 to the DPDP Act, 2023.* *African Journal of Biomedical Research.* Retrieved from: https://africanjournalofbiomedicalresearch.com/index.php/AJBR/article/view/176 7
10. Author Unknown. (2025). *A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India.* SSRN Working Paper. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm? abstract_id=5335388
11. Bhasin, P. (2025). *Practical Guide to Digital Personal Data Protection Act, 2023 – Law and Compliance.* New Delhi: OakBridge Publications.
12. Nayyar, Y. V. (2026, 2nd ed.). *The Digital Personal Data Protection Act, 2023.* New Delhi: EBC / Whitesmann Publications.
13. Bhandari, M. K. (2025). *Digital Personal Data Protection Act, 2023 – A Commentary and Compliance Guide.* New Delhi: Eastern Book Company (EBC).
14. Corporate Professionals. (2026). *Handbook on the Digital Personal Data Protection Act, 2023.* New Delhi: Commercial Law Publishers (India) Pvt. Ltd.
15. Commercial Law Publishers. (2025). *The Digital Personal Data Protection Act, 2023 – E-Book Edition.* New Delhi: Commercial Law Publishers (India) Pvt. Ltd.
16. Corporate Professionals. (2025). *The Digital Personal Data Protection Act, 2023 – A Practical Compliance Workbook.* New Delhi: Commercial Law Publishers (India) Pvt. Ltd.
17. Tandon, U., & Gupta, N. K. (2025). *Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023.* *Law in Depth*, 12(2), 87–117.
18. Saha, S. (2024). *A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023.* *International Journal of Law and Society*, 10(1). Retrieved from: https://www.journalsalliancepub.com/index.php/ijls/article/view/114
19. Viswanathan, S. T. (2023). *Indian Cyber Law and Digital Governance.* New Delhi: PHI Learning.
20. Mani, K. (2025). *Cyber Law and Data Protection in India – A Student-Friendly Text.* Chennai: G. G. Gopalakrishnan Publishers.
21. Pandey, R. N. (2025). *Commentary on the Information Technology Act, 2000 (with DPDP Act, 2023 and Amendments).* New Delhi: Mandling & J. Services.
22. Barowalia, J. N., & Barowalia, A. (2022). *Commentary on the Information Technology Act, 2000 (with Rules, Regulations, and Notifications).* New Delhi: Eastern Book Company (EBC).
23. Kalra, K., & Aggarwal, S. (2024). *Commentary on the Information Technology Act, 2000 (2nd ed.).* New Delhi: Whitesmann Publications.
24. Duggal, P. (Latest ed.). *Cyberlaw in India.* New Delhi: Wiley India / Saakshar Law Publications.
25. Reed, C. (2023). *Information Technology Law and Practice.* Oxford: Oxford University Press.
26. Chander, H. (2022). *Advanced Cyber Law and IT Protection.* New Delhi: PHI Learning.
27. Sharma, V. (2021). *Cyber Law and Practice – Foundations and Applications.* New Delhi: Eastern Law House.
28. Gupta, A. (2020). *Commentary on the Information Technology Act, 2000 (with Case Law).* New Delhi: Universal Law Publishing.
29. Lloyd Law College. (2026). *Data Protection Laws in India: A Complete Guide for 2026.* Retrieved from: https://www.lloydlawcollege.edu.in/blog/ data-protection-laws-india-2026-guide.html
30. PRS India. (2026). *The Digital Personal Data Protection Bill, 2023 – Bill Track and Policy Analysis.* Retrieved from: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
31. Carnegie Endowment for International Peace. (2023). *Understanding India's New Data Protection Law (DPDP Act, 2023).* Retrieved from: https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law
32. Lawyers Worldwide. (2024). *Digital Personal Data Protection Act, 2023 – Commentary and*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Practical Guide.
Retrieved from: https://www.lawyersworldwide.com/wp-content/uploads/Digital-Personal-Data-Protection-Act-2023.pdf

33. Mayer Brown LLP. (2025).
India's New Privacy Law Is Here: What You Need to Know.
Retrieved from: https://www.mwe.com/insights/what-to-know-about-indias-new-privacy-law/

34. JDSupra. (2026).
India's New Data Privacy Rules Are Here: 8 Steps for Compliance under the DPDP Act, 2023.
Retrieved from: https://www.jdsupra.com/legalnews/india-s-new-data-privacy-rules-are-here-3965275

35. Author Unknown. (2025).
Critical Analysis of the Digital Personal Data Protection Act, 2023. International Journal of Law, Letters and Research (IJLLR). Retrieved from: https://www.ijllr.com/post/critical-analysis-of-the-digital-personal-data-protection-act-2023

36. Commercial Law Publishers. (2025). *The Digital Personal Data Protection Act, 2023 – Bare Act with Short Notes (2025 Edition).*
New Delhi: Commercial Law Publishers (India) Pvt. Ltd.

37. BPB Online. (2025).
The Digital Personal Data Protection Act: A Practitioner's Guide for Compliance and Audits.
New Delhi: BPB Publications.

38. Corporate Professionals. (2026).
The Digital Personal Data Protection Act, 2023 – A Practical Compliance Workbook (2nd Edition).
New Delhi: Commercial Law Publishers (India) Pvt. Ltd.

39. Government of India. (2023).
The Digital Personal Data Protection Act, 2023 – Official Gazette Notification and Text.
Retrieved from: https://www.indiacode.nic.in/handle/123456789/22037

40. Press Information Bureau, Government of India. (2025).
Government notifies DPDP Rules to empower citizens and support innovation (2025 update).
Retrieved from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014