



An Analysis of Digital Personal Data Protection Act, 2023 and Intellectual Property Rights

Chetankumar T M

Assistant Professor,
Raja Lakhamgouda Law College,
Tilakwadi, Belagavi – 590006.
Karnataka.

Dr. Rajendra kumar Hittanagi

Assistant Professor and Research Guide
Karnataka State Law University,
Navanagar, Hubballi – 580025.

Abstract

Over the past ten years, India has experienced an unthinkable surge in the digital world due to the quick adoption and expansion of social media, online platforms, e-commerce, and most recently, online payment methods. Concerns about it increased along with its simplicity of use and the abundance of features that make life easier. People began to experience privacy violations, security problems, and data breaches, among other things. The main issue was that there was no explicit legislation governing the use of data in the digital sphere. The necessity for a legislative framework to protect digital data increased after the Supreme Court of India declared that privacy was a fundamental right. India's digital economy is experiencing an extraordinary increase in data-driven innovation, encompassing AI-enhanced services and inventive digital content. In conjunction with this expansion, two essential legal frameworks regulate the management of information and ideas; data protection law and intellectual property (IP) law. These frameworks fulfill distinctly different roles; one is designed to protect personal information and privacy, while the other safeguards intellectual creations. However, they are increasingly overlapping and even conflicting in the realm of contemporary technology. A critical examination of the differences between data protection and IP law in India, elucidating each within the Indian context, comparing their goals and mechanisms, and investigating how they intersect, clash, and can be strategically navigated within the digital and AI economy. Relevant Indian legislation, such as the Digital Personal Data Protection Act, 2023 (DPDPA), the Patents Act, 1970, and the Copyright Act, 1957, are analyzed to offer practical guidance for businesses, startups, creators, and individuals operating in India.

Keywords: Technology, Development, Digital Protection, Data laws, IP laws.

Introduction

The world is abundant with data. The proliferation of big data, analytics, and artificial intelligence (AI) has led to the emergence of numerous new information-rich services, as well as the transformation of existing companies. Data contributes, among other factors, to wealth and economic value. Organizations are discovering methods to extract value from data, and frameworks are being established to enhance the understanding of data's applications and advantages. Due to the increasing importance of the data economy and its potential for value creation, governments worldwide are recognizing the necessity of facilitating and regulating all aspects of data, encompassing both personal and non-personal data.

Data protection is essential as it safeguards the private information of individuals or organizations against any act such as identity theft, hacking, fraud and phishing attacks. Any organizations aiming for efficient operation establish a data protection strategy to ensure the safety of its information. Data protection refers to the practice of safeguarding sensitive information from being lost, altered, or damaged. As data is generated and saved at unparalleled speeds, data security is increasingly crucial. Ensuring that data can be quickly recovered after any corruption or loss forms a crucial part of a data protection plan. Additional vital components of data protection involve ensuring data confidentiality and safeguarding data from breaches.

Big data and data analytics are two terms that collectively define big data analytics. This concept refers to data sets that are rapidly increasing in size and encompass substantial amounts of intricate data. Data analytics involves the examination of data to derive valuable insights through various methods or tools. Analytics is employed to address challenges and enhance the efficiency of multiple sectors¹. The advancement of the Banking, Financial Services, and Insurance (BFSI) sector is significantly reliant on analytics. By collecting and analyzing healthcare data from wearable smart devices and Electronic Medical Records (EMR), it is also transforming the healthcare sector. This plays a crucial role in preventive healthcare by facilitating the early detection of numerous diseases.

Nevertheless, large data sets necessitate extensive storage, a range of tools and technologies, and a considerable budget for management and analysis. Organizations encounter significant challenges in managing and storing this type of data, as most big data tools collect and analyze data in real-time. Furthermore, if the data volume increases exponentially, scalability becomes an issue. That said, the most significant threat to data is security breaches. In 2022, India was ranked second worldwide in terms of data breaches. Therefore, strong protection measures are essential. Implementing best practices alongside stringent legal enforcement is the pathway to effective data protection.

Data Protection in India - Background

India has entered a new phase regarding data protection. Until now, we have depended on the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) as the sole legislations for interpreting all matters related to data². The initial attempt to safeguard data can be traced

¹ *Data Protection- the regime in India (Part-I)*

https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/data-protection-regime-india-part-i-2024-01-04_en

² Vatsal Gaur and Krishnan Sreekumar, A DAWN OF A NEW ERA FOR DATA PROTECTION IN INDIA: AN IN-DEPTH ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
August 15, 2023

<https://www.legal500.com/developments/thought-leadership/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysis-of-the-digital-personal-data-protection-act-2023/>

back to an amendment to the Information Technology Act, 2000 (IT Act) in 2008³. This amendment established a requirement for companies to protect any sensitive personal data and information they possess, manage, or interact with on a computer resource by implementing and maintaining suitable security measures. Additionally, it imposed penalties for non-compliance.

Following this, a rule was introduced in 2011⁴ that outlined the minimum standards for the protection of sensitive personal data. This included mandates for businesses to establish a privacy policy, obtain consent prior to collecting or transferring sensitive personal data, and inform individuals about the recipients of such data.

As information technology industry experienced rapid growth, various sector-specific rules and regulations were implemented. Incorporating remedies and preventive measures aimed at data protection. Nevertheless, this fragmented development resulted in gaps and inconsistencies within the data protection framework, highlighting an urgent need for a comprehensive law and enforcement mechanisms⁵.

India's legal framework for data protection began with the landmark Supreme Court ruling in Justice *K.S. Puttaswamy (Retd.) v. Union of India*⁶, which declared the right to privacy as a constitutional right under Article 21 of the Constitution. The Court highlighted that privacy is fundamental to individual freedom and established the proportionality test for any limitations. This ruling established constitutional foundations for a robust data protection framework that shaped the essential elements of the Digital Personal Data Protection (DPDP) Act, 2023, including informed consent, data minimization, and individual rights concerning personal data⁷.

- The DPDPA facilitates the processing of digital personal data while ensuring the protection of individual's privacy rights and the necessity of processing such data for legitimate reasons. This legislation outlines the responsibilities of individuals, corporations, and governmental bodies that handle data, as well as the rights and obligations of the individuals to whom the data pertains.

³ Section 43A of the IT Act

⁴ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

⁵ *Data Protection- the regime in India (Part-I)*

https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/data-protection-regime-india-part-i-2024-01-04_en

⁶ AIR 2017 SC 4161

⁷ Mr. Ketan Joshi, NAVIGATING THE DIGITAL DATA REGIME: AN ANALYSIS OF THE DPDP ACT & DPDP RULES 2025

May 8, 2025

<https://www.legal500.com/developments/thought-leadership/48168/>

- The DPDPA aims to establish a robust data protection framework with minimal disruption to the data-driven society, thereby improving the quality of life and simplifying business operations by fostering an innovation-centric environment.
- The DPDPA guarantees an individual's right to access information regarding their personal data that is being processed. It also ensures the right to correct and delete such data.
- The DPDPA applies not only to India citizens and companies that collect data from Indian citizens but also to non-citizens residing in India. Furthermore, it regulates the processing of data collected in India related to any activities that involve providing goods or services outside of India. For example, the DPDPA would be relevant even if a service provider located outside of India offers digital goods or services to a French citizen residing in India.
- The DPDPA authorizes the processing of personal data for any legitimate purpose, which is explicitly detailed in the statute. The entity or party responsible for managing such data may proceed with the consent of the individual concerned or for "legitimate purposes"⁸.
- In instances of violations, the DPDPA provides for more severe penalties and the imposition of substantial fines. These fines are punitive rather than compensatory in nature.
- Additionally, the DPDPA outlines provisions for electronically mediated alternative dispute resolutions, which, according to the statute, would be activated in the event of a dispute or disagreement.
- Furthermore, the DPDPA grants the government the authority to limit public access for repeat offenders to any information, including websites and applications, that could be used by data fiduciaries for marketing goods and services⁹.

The significance of privacy and data protection is being recognized more and more, as more social economic activities shift online. 137 out of 194 nations have passed legislation to guarantee data and privacy protection in response to data protection and privacy. Some nations¹⁰ have data protection laws in place to safeguard their citizen's privacy and data¹¹.

⁸ Sections 7 and 17 of THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

⁹ *Data Protection- the regime in India (Part-II)*

https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/data-protection-regime-india-part-ii-2024-01-04_en
Accessed on 18-08-2025 at 12:00 AM

¹⁰ **European Union** - General Data Protection Regulation

China - China Personal Information Protection Law

South Africa - Protection of Personal Information Act

Japan - Act on the Protection of Personal Information

Australia - Privacy Act 1988

New Zealand - Privacy Act 2020

¹¹ *Evolution of Digital Personal Data Protection Law in India*

Digital Personal Data Protection Law and Intellectual Property Rights

The importance of Intellectual property in society has grown dramatically as a result of the digital age's quick development. The development of software, digital material, new technologies, etc, depends heavily on intellectual property. When personal data is used in such inventions, the DPDP Act is applicable.

The Digital Personal Data Protection (DPDP) Act, 2023, intends to safeguard individuals' digital personal data while allowing for its legal processing. Although not explicitly aimed at intellectual property rights (IPR), the Act's regulations on data consent, transparency, and security may have an indirect influence on IPR. For example, the DPDP Act's stipulations for securing consent prior to the collection and processing of data can apply when handling personal data connected to intellectual property, like user data for online games or software applications. Likewise, the Act's focus on data protection and preventing breaches can safeguard intellectual property against unauthorized access and disclosure. There are several situations in which compliance with the DPDP Act is necessary when developing intellectual property (IP):

- If personal data is involved in the creation of any intellectual work, such as the development of algorithmic software, it is essential to adhere to the provisions of the DPDP Act.
- In cases where licensing of personal data is needed for research, innovation, or business purposes, the privacy safeguards outlined in the DPDP Act must be observed.
- When personal data is included in a copyrighted work, the creation will be protected under copyright law, while DPDP Act safeguards the data contained within it, including personal identifiers such as names, addresses, and biometric information.
- Trade Secrets represents a significant area of intersection between IP and the DPDP Act. While trade secrets are generally protected under IP legislation, any sensitive personal data, including confidential algorithms, databases, and lists containing names and other personal information, is legally protected under the DPDP Act.
- International collaboration in IP often involves the sharing of personal data. For instance, if individuals from different countries collaborate on any form of IP creation, such as innovation or research, the shared data must comply with the DPDP Act. The DPDP Act governs cross-border data transfers and ensures that any personal data shared internationally meets Indian privacy standards.

India's intellectual property legislation establishes a comprehensive structure to safeguard mental creations – inventions, artistic and literary works, trademarks, designs, and others. In contrast to data protection (focused on personal rights), IP law establishes property rights in intangible assets, enabling creators or inventors to possess and benefit from their inventions. India has a broad IP framework, encompassing laws related to patents, copyrights, trademarks, industrial designs, semiconductor layouts, plant varieties, and more. In this context, the most pertinent areas concerning digital and AI are patents and copyrights¹².

The interaction between the IP and DPDP Act presents a distinct array of challenges. The DPDP Act requires informed consent for any form of data utilization. This requirement may hinder innovations or research that depends on datasets. The rise and expansion of Artificial Intelligence, which encompasses both personal data and creative works, introduce specific challenges, particularly regarding ownership issues. The legal framework, to a certain degree, assists in aligning data protection with IP considerations, thereby minimizing conflicts.

The DPDP Act offers a systematic approach to data protection in India. It was established to enable India to prosper in the global digital economy without compromising on data breaches and other privacy and security issues. It is essential to achieve a balance between the DPDP Act and IP laws to safeguard privacy while encouraging new creations and innovations. Individuals who aim to create intellectual property must ensure compliance with both legal frameworks. Creators, authors, inventors, and others can protect the proprietary rights of their creations without compromising data protection¹³.

Conclusion

Data protection and intellectual property law exhibit nearly opposite orientations; the former regulates and limits the use of personal information to safeguard individual rights, whereas the latter confers exclusive rights to promote the utilization of innovative or creative works. Both are crucial, as privacy law cultivates a reliable digital environment, while IP law incentivizes innovation. However, their intersection can be quite intricate, particularly in areas such as digital technology and artificial intelligence, where substantial quantities of data (often personal) are employed to generate valuable intellectual property. This necessitates a careful equilibrium.

Navigating this dual landscape is undoubtedly challenging, yet it also presents an opportunity. Businesses that successfully leverage data in an ethical and legal manner are likely to gain increased user trust and encounter fewer legal obstacles. For instance, an AI company that utilizes only consented or

¹² *Data Protection v. Intellectual Property in India's Digital and AI Era*
<https://www.boudhikip.com/data-protection-vs-intellectual-property-in-indias-digital-and-ai-era/>

¹³ Shwetha, *Digital Protection and Intellectual Property- An interplay*
<https://www.puthrans.com/digital-protection-and-intellectual-property-an-interplay/>

anonymized data and honors content rights will experience a more straightforward path compared to one that finds itself in litigation with privacy regulators or copyright holders. Similarly, creators who honor privacy in their content and innovators who respect the intellectual property of others will contribute to a more collaborative and sustainable digital ecosystem, even as they utilize the law to protect their own rights. As India's Digital Personal Data Protection Act, 2023 is implemented and IP laws evolve in response to new technologies, the underlying principle remains balance. As articulated in one analysis, companies must "proceed cautiously to leverage big data for technological advancements while adhering to privacy regulations," all while safeguarding their ideas without "infringing on the rights of others." Attaining this balance requires viewing compliance not as a burden, but as an integral component of corporate strategy and innovation design.

Reference

1. *Digital Protection and Intellectual Property- An interplay*
<https://www.puthrans.com/digital-protection-and-intellectual-property-an-interplay/>
2. *Data Protection v. Intellectual Property in India's Digital and AI Era*
<https://www.boudhikip.com/data-protection-vs-intellectual-property-in-indias-digital-and-ai-era/>
3. *Data Protection- the regime in India (Part-I)*
https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/data-protection-regime-india-part-i-2024-01-04_en
4. Gaur Vatsal and Sreekumar Krishnan, A DAWN OF A NEW ERA FOR DATA PROTECTION IN INDIA: AN IN-DEPTH ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
August 15, 2023
<https://www.legal500.com/developments/thought-leadership/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysis-of-the-digital-personal-data-protection-act-2023/>
5. *Data Protection- the regime in India (Part-I)*
https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/data-protection-regime-india-part-i-2024-01-04_en
6. Mr. Joshi Ketan, NAVIGATING THE DIGITAL DATA REGIME: AN ANALYSIS OF THE DPDP ACT & DPDP RULES 2025
May 8, 2025
<https://www.legal500.com/developments/thought-leadership/48168/>
7. *Evolution of Digital Personal Data Protection Law in India*
<https://www.manupatracademy.com/assets/pdf/legalpost/evolution-of-digital-personal-data-protection-law-in-india.pdf>

8. *Data Protection v. Intellectual Property in India's Digital and AI Era*
<https://www.boudhikip.com/data-protection-vs-intellectual-property-in-indias-digital-and-ai-era/>
9. Shwetha, *Digital Protection and Intellectual Property- An interplay*
<https://www.puthrans.com/digital-protection-and-intellectual-property-an-interplay/>

