INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

IMPACT OF THE DIGITAL PERSONAL DATA PROTECTION ACT ON COPYRIGHT AND PRIVACY RIGHT

AUTHOR – VARUN LOHIA* & SHUBHAM KUMARI**

STUDENT AT AMITY UNIVERSITY PATNA

BEST CITATION - VARUN LOHIA & SHUBHAM KUMARI, IMPACT OF THE DIGITAL PERSONAL DATA PROTECTION ACT ON COPYRIGHT AND PRIVACY RIGHT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (14) OF 2025, PG. 278-281, APIS – 3920 – 0001 & ISSN - 2583-2344.

I. Introduction: The Legislative Fulcrum of Digital Governance

The enactment of the Digital Personal Data Protection Act 2023 (DPDP Act)[220] signifies a development in Indias digital regulatory landscape establishing the nations inaugural all-encompassing framework for managing the handling of digital personal data. This legislation, passed by Parliament on August 11 2023 is not merely a regulation—it embodies the constitutional realization of the Supreme Court's pivotal decision, in Justice K.S. Puttaswamy (Retd.). Anr.. Union of India and Ors. (2017)[221] Which ruled that privacy is an essential element of the fundamental right to life guaranteed by Article 21 of the Constitution of India. Acknowledging privacy as a right intensified the need for a strong rights-focused framework, for data governance leading to the DPDP Act serving as the legislative tool to fulfill that constitutional requirement.

[220] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[221] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017) 10 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The Act is founded on seven principles - consent, purpose limitation, data minimization, storage limitation, transparency, accountability and security each aimed at reconciling technological progress with personal autonomy. Clear operational guidelines were subsequently introduced through the Digital Personal Data Protection Rules, 2025 along with the creation of the Data Protection Board (DPB) which currently serves as the authority responsible, for enforcement, penalties and dispute resolution.

This legislative transformation brings consequences for related legal frameworks, especially Intellectual Property (IP) law. Before the DPDP Act disputes involving the overlap of privacy and copyright protection were mainly handled under the Information Technology Act, 2000 through contractual agreements or, via sector-specific technological measures. As privacy evolves into a guaranteed right data processing operations integral to IP-based commercial frameworks including content customization, Digital Rights Management (DRM) anti-piracy monitoring and AI-driven content generation are required to pass the constitutional criteria of necessity, proportionality and legality set forth in Puttaswamy. Therefore India is now confronted with a legal challenge: harmonizing privacy as a fundamental right, with the statutory aim of copyright law to promote creativity, safeguard authors and uphold the market value of creative works.

II. Statutory Definitions and the Consent-Centric Paradigm

The DPDP Act establishes a governance framework centered on rights granting recognition to those involved in data processing. The Data Principal is the person to whom the personal data pertains. The Data Fiduciary is the organization either governmental that decides the objectives and methods of processing. Moreover some organizations are classified as Significant Data Fiduciaries (SDFs) due to factors, like size, sensitivity, national security or public interest concerns obliging them to designate a Data Protection Officer (DPO) perform Data Protection Impact Assessments (DPIAs) and implement technical protections.[222]

The Act governs processing carried out inside India well as outside its borders by entities managing personal data of persons situated in India while providing goods or services. Consent is the basis for lawful processing, characterized as voluntary precise, knowledgeable, clear and unconditional requiring explicit positive action marking a definite departure, from previous methods involving combined, ambiguous or default consent frameworks.

III. Identifying the Legal Intersection: Privacy Rights vs. Intellectual Property Rights (IPRs)

The tension between privacy and intellectual property law arises when personal information is incorporated into or essential, for the development, application and protection of IP assets. This appears mainly in two areas:[223]

Area Privacy Conflict Example

IP Creation AI model training using scraped datasets with personal data, commercial databases, algorithm development

IP Enforcement Collection of metadata, user logs, device identifiers, and behavioural tracking for anti-piracy enforcement

Therefore the IP owner must regard data simultaneously as a valuable commercial resource and a legally safeguarded responsibility, under DPDP transforming all conventional data-centric business approaches.

IV. Codification of Privacy Rights and New Compliance Duties[224]

A. Consent and Purpose Limitation

[222] Decoding the Digital Personal Data Protection Act, 2023 - EY.
[223] Effective Applicability of Sections 65A and 65B of Copyright (Amendment) Act, 2012 using Case Study of Digital Watermarks - Manupatra.
[224] DPDPA's Global Reach: Cross-Border Data, AI Impact, and International Alignment.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The Act mandates that data must be utilized solely for the reason consent was originally obtained. Any additional use such, as analytics, algorithm improvement or behavioural profiling demands new consent. This dismantles the commercial approach of unlimited data monetization.

B. Data Principal Rights

Data Principals are now entitled to rights including access, rectification, deletion and the revocation of consent. These rights generate conflict when personal information is fundamentally embedded within copyright-protected entities like AI models or databases. The right to deletion is especially challenging when personal data serves as evidence, in copyright dispute cases.

C. Legitimate Uses under Section 7

In contrast to GDPR the DPDP Act does not include 'legitimate interests and 'contractual necessity' as lawful bases for processing. This exclusion places a responsibility on IP owners who earlier depended on legitimate interest balancing tests, for monitoring enforcement.

V. Data Privacy Challenges to Copyright Enforcement and Digital Rights Management (DRM)

A. Erasure-Retention Conflict

Copyright[225] disputes depend significantly on preserved metadata such as timestamps, device information, location and IP addresses. However according to Section 12 data must be deleted once its purpose is fulfilled or consent is revoked. There is no legal guidance on whether retaining data for litigation qualifies, as a legitimate overriding public interest.

B. DRM Conflicts with Data Rights

Custom watermarks employed for tracking might include personal identifiers. Removing or modifying them could potentially violate Section 65B of the Copyright Act.

VI. Impact on AI / ML, Fair Dealing, and Text and Data Mining[226]

AI training generally depends on collecting data to the public. According to DPDP obtaining consent is mandatory for data and the 'public availability' exception does not cover copyright protection. India does not have judicial guidance, on whether TDM falls under Section 52's fair dealing. As a result AI creators encounter legal risks: breaches of privacy and intellectual property violations.

VII. Intermediary Liability and Harmonized Due Diligence

According to Section 79 of the IT Act intermediaries receive protection from liability concerning third-party content. Compliance, with DPDP is now part of diligence—neglecting to protect personal data can void safe harbour and subject platforms to allegations of contributory copyright infringement.

VIII. Policy Reform Recommendations

In order to harmonize the requirements of copyright enforcement with the privacy-focused objectives of the Digital Personal Data Protection Act, 2023 specific policy adjustments are crucial to create clear regulations and effective enforceability. Initially the Government must explicitly define litigation-related data retention as a purpose under the Act allowing limited retention of metadata strictly essential for copyright enforcement and court processes contingent, on proportionality and oversight measures. Second, there is an urgent need to develop privacy-neutral Digital Rights Management (DRM) standards, transitioning from identity-linked tracking mechanisms to cryptographically anonymized watermarking and non-personalized evidence trails capable of proving infringement without exposing user identities. Third consistent with frameworks like the EU's DSM Directive India ought to implement regulated AI training and text-and-data mining (TDM) exceptions within Section 52 of the Copyright Act, 1957 allowing non-expressive

[225] The Copyright Act, 1957 (Act 14 of 1957), s. 52.

[226] 'Fair Use' in the Age of AI | India Corporate Law.

non-derivative computational examination, under opt-out options, protected environments and transparency requirements. Moreover a consolidated due diligence framework for platforms needs to be created via collaborative directives from MeitY, the Data Protection Board and the Copyright Office setting uniform compliance standards related to notice-and-takedown repeat infringer rules and privacy-conscious evidence retention. Lastly specific regulatory exemptions, for creative sectors should be designed to foster innovation acknowledging the unique economic sensitivities of artistic groups and permitting reasonable data utilization to protect intellectual property while upholding robust privacy safeguards. Together, these reforms would enable harmonized digital governance, balancing innovation incentives, creator rights, and the constitutional right to informational privacy[227].

IX.CONCLUSION

The DPDP Act embodies Indias effort to enshrine autonomy into law and restore authority over personal data to individuals. Meanwhile the Copyright Act stands as the foundation of India's creative and digital sectors. The areas of friction between these two laws are neither coincidental nor fleeting they reveal a philosophical clash between privacy as an extension of identity and intellectual property, as a driver of economic motivation.

Of selecting one option at the expense of the other Indian legislation should craft a balanced framework that upholds constitutional privacy alongside supporting innovation and effective copyright protection. This path forward involves privacy-, by-design DRM systems, defined processing exceptions and unified legal standards.

If India can successfully reconcile these interests, it can emerge as a global model for democratic digital markets—protecting creators without compromising citizens.

[227] Online Copyright Infringement and Its liability Upon Intermediary.