Page 1800 - 1829 **DOI:** *https://doij.org/10.10000/IJLMH.115001*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 3

2023

The Interface Between Data Protection and Intellectual Property Laws

PRIYA GUPTA[1] AND AFREEN KHAN[2]

ABSTRACT

"The rapid growth of digital technologies and the Internet has revolutionized the way people communicate, share, and consume information. This transformation has brought forth new challenges in the realms of data protection and IPR. The present dissertation provides a comprehensive analysis of the legal frameworks governing data protection and IPR in India, as well as their intersection and the challenges arising therefrom.

This paper will examine the legal framework for data protection in India. The focus is on the IT Act, 2000, and its associated rules and regulations, including the recent DPDP Bill, 2019, is also discussed, emphasizing its key provisions and the changes it aims to bring to the existing data protection landscape. Further, the dissertation addresses the enforcement mechanisms and the role of the proposed Data Protection Authority in ensuring compliance with the data protection laws.

Further this paper will discuss the proceeds to examine the interface between data protection and IPR, focusing on the overlapping concerns and challenges that arise in this context. Areas of overlap include database protection, technological protection measures (TPMs), trade secrets and confidential information, RMI, and user-generated content on social media platforms. The dissertation analyzes the legal issues surrounding these areas, incorporating relevant case laws and international comparisons to provide a comprehensive understanding of the challenges at the intersection of data protection and IPR".

Overall, this paper contributes to the ongoing discourse on data protection and IPR in India, highlighting the need for a robust and adaptable legal framework that addresses the evolving challenges in the digital age. By taking into account the complexities at the intersection of data protection and IPR, India can foster a thriving digital ecosystem that respects both IPR and data protection principles while promoting innovation and creativity".

Keywords: *Data, Protection, Rights, IPR, Digital Media.*

[1] Author is a LL.M. student at AIALS, Amity University, India.
[2] Author is a LL.M. student at AIALS, Amity University, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The "concept of data security and privacy may have originated in ancient Indian civilisation when personal information protection was woven into the moral and cultural fabric. However, the legal acknowledgment of the right to privacy and data protection in India started with the adoption of the Indian Constitution in 1950. Although the right to privacy is not directly stated in the Constitution, many clauses, such as Article 21 (right to life and personal liberty) and Article 19(1)(a) (right to freedom of speech and expression), provide the groundwork for it.

The Supreme Court of India recognised the right to privacy as an essential part of Article 21 in the landmark decision Kharak Singh v. State of Uttar Pradesh[3] . Despite its recognition, the extent of privacy as a basic right remained unclear for many years.

During the pre-IT period, the legal framework addressing data protection was dispersed among numerous legislations, including the Indian Evidence Act of 1872, the Indian Telegraph Act of 1885, and the Indian Penal Code of 1860 (IPC), with a concentration on physical forms of data. Personal data is only partially protected under these restrictions, which are primarily concerned with preventing unauthorised access, interception, and dissemination[4].

(A) Post-IT Era

As a result of the entry of the IT age in India, which was marked by economic liberalisation in the 1990s and the rapid expansion of the internet and digital technologies, a comprehensive legal framework is required to address data protection and privacy issues in the digital sphere.

The IT Act, 2000 was the first legislation in India to particularly address concerns of data protection and privacy in the context of electronic commerce and communication." The major goals of the IT Act were to promote e-commerce, simplify electronic transactions, and combat cybercrime. However, it did not go into great length on privacy and data protection problems.

Sections 43A and 72A of the IT Act were added in 2008 to incorporate safeguards for data protection and privacy. Section 43A holds a firm liable for compensating persons who suffer unjust loss or gain as a consequence of carelessness in developing and implementing proper security practises and procedures. Section 72A prohibits the dissemination of personal information received under a valid contract without the agreement of the data subject with the goal of inflicting unlawful damage or obtaining an unfair advantage.

Despite these changes, the IT Act does not establish a comprehensive framework for data

[3] (1963) AIR 1295

[4] "Sodhi, Bansari Samant and Tushar Sinha, 'The Journey of India's Data Protection Jurisprudence', *available at*: https://www.lexology.com/library/detail.aspx?g=57720842-f709-4dd4-947b-44c3c6e4ed10

 [ISSN 2581-5369]

security. To remedy this gap, the Justice B.N. Srikrishna Committee was formed in 2017, and the DPDP Bill was drafted in 2019. The European Union's General Data Protection Regulation (GDPR) and other international rules serve as the basis for the PDP Bill, which intends to build a strong data protection framework in India.

The DPDP Bill, which is now being debated in Parliament, establishes a comprehensive framework for the collection, storage, processing, and disclosure of personal data. It defines terms such as 'data fiduciaries,' 'data processors,' 'data localization,' and 'data protection officers.' The PDP Bill also proposes the Data Protection Authority of India (DPAI), a new independent regulatory organisation in charge of regulating and implementing the nation's data protection system.

II. LEGAL FRAMEWORK

(A) Constitutional Provisions

The Indian Constitution, which is the ultimate law of the nation, serves as the foundation of India's legal framework controlling data privacy. Although the right to privacy and data protection are not specifically addressed in the Constitution, they are mentioned multiple times, most notably in the context of basic rights.

a. Article 21: Right to Life and Personal Liberty

Article 21 of the Constitution protects the right to life and personal liberty, stating that neither right may be compromised unless done so in accordance with the law. The Supreme Court of India has added the right to privacy to Article 21 as a fundamental feature of individual freedom throughout time[5].

In Justice *K.S. Puttaswamy v. Union of India* [6], the Supreme Court recognized "the right to privacy as a fundamental right guaranteed by Article 21. In this judgement, the Supreme Court's nine-judge panel unanimously decided that Article 21's guarantee for the right to privacy is an integral component of the rights to life and personal liberty. The Court further said that privacy encompasses informational privacy, which involves both the protection of personal data and the control that persons have over such data.

The Puttaswamy case has had a major influence on India's data protection debate, underlining the necessity for a comprehensive legislative framework that protects people' privacy rights in the digital era.

[5] The Constitution of India, art. 21.
[6] (2017) 10 SCC

 [ISSN 2581-5369]

b. Article 19(1)(a): Right to Freedom of Speech and Expression

According to Article 19(1)(a) of the Constitution, all people enjoy the right to free speech and expression. This right has been construed to encompass the freedom to access and distribute information, which is inextricably tied to DPDP and privacy.

The Supreme Court said in *Cricket Association of Bengal v. Secretary, Ministry of Information and Broadcasting*[7], Government of India that freedom of speech and expression includes the right to seek information and ideas without impediment. As the free flow of information is so important in a democratic society, this right applies not only to the speaker or sender of information, but also to the receivers of such information.

The link between free speech and data protection is especially essential in the context of the internet and digital technology, where the free flow of information is both a facilitator and a possible danger to people's private rights.

c. Other Constitutional Provisions

Articles 21 and 19(1)(a) of the Indian Constitution, among others, have an impact on India's legislative framework for data protection." Article 300A, for example, guarantees the right to property, which might be interpreted to encompass a person's intellectual rights in their personal data[8].

Furthermore, "Articles 14 (right to equality) and 15 (prohibition of discrimination) are significant in the context of data protection As they require the state to ensure that the collection, processing, and disclosure of personal data does not result in discriminatory practises or violate the principles of equality and non-discrimination.

(B) Proposed Legal Reforms

To address the difficulties of the digital age, the Indian government has launched a variety of measures to modify current laws and create new legislation. This is done in awareness of the necessity for India to have a comprehensive and strong legislative framework for data protection. To increase data privacy in India, the following essential legislative amendments have been proposed:

(C) DPDP Bill, 2022 (DPDP Bill)

The PDP Bill, 2022, is a key piece of legislation with the purpose of creating a comprehensive data protection framework in India. The European Union's General Data Protection Regulation

[7] (1995) 2 SCC 161
[8] The Constitution of India, arts. 19(1)(a).

 [ISSN 2581-5369]

(GDPR), which is heavily influencing the Bill currently before Parliament, intends to address a variety of data protection concerns, including consent, data localization, cross-border data transfers, and data fiduciary requirements[9].

The following are some of the important provisions of the DPDP Bill:

- Data Principal Rights: The Bill grants people (known as 'data principals') a variety of personal data rights, including the right to access, correction, deletion, and portability.
- Responsibilities of Data Fiduciaries: The DPDP Bill imposes stringent requirements on enterprises that collect, handle, and preserve personal data (also known as 'data fiduciaries'), including the need to get permission, follow privacy-by-design principles, and appoint a data protection officer".
- Data Localization: "The Bill requires that some categories of personal data be kept only in India and authorises the transfer of other categories of data in specific circumstances.

The DPDP Bill proposes an independent regulatory organisation, the Data Protection Authority of India (DPAI), to be in charge of implementing and enforcing the nation's data protection policy.

(D) Amendments to the IT Act, 2000

In view of the evolving digital world and the growing emphasis on data protection, there has been talk about updating the IT Act of 2000 to meet modern challenges and reinforce the extant legal framework. Among the predicted changes are the following[10]:

- Improving data security, privacy, and secrecy in accordance with the DPDP Bill's guiding principles.
- To create a greater deterrence to offenders, the punishment for breaking data privacy rules should be increased.
- incorporate legislation for cutting-edge technologies like as blockchain, artificial intelligence, and machine learning, all of which have a significant impact on data security.

(E) Data Empowerment and Protection Architecture (DEPA)

The RBI's National Strategy for Financial Inclusion 2019-2024 recommends the creation of a Data Empowerment and Protection Architecture (DEPA). DEPA aspires to build an ecosystem

[9] "Charanya Lakshmikumaran, 'Digital Personal Data Protection Bill: What rights does it give individuals?' *The Economic Times*."
[10] "Yashraj Bais, 'Privacy and Data Protection in India: An Analysis,' 4 *IJLMH 51 (*2021)."

 [ISSN 2581-5369]

that gives people more control over their personal data and allows them to exchange it in a safe and informed way with data fiduciaries. The design attempts to stimulate data-driven innovation while protecting data security and privacy.

(F) Non-Personal Data Governance Framework

In addition to preserving personal data, the government has begun to take efforts to manage non-personal data, which is defined as material that does not directly or indirectly identify persons. In 2019, a panel of experts headed by Kris Gopalakrishnan convened to examine numerous non-personal data-related concerns and suggest an appropriate governance system." The committee's report, due in 2020, proposes the establishment of a regulating body for non-personal data, as well as a variety of initiatives for capitalising on the economic potential of such data while respecting people' privacy.

III. LEGISLATION AND REGULATIONS

(A) IT (Amendment) Act, 2008

The IT (Amendment) Act of 2008 [11]"brought a number of significant revisions to the IT Act of 2000 , with the primary goal of addressing emerging digital problems and creating a legal framework for electronic transactions, e-governance, and data security. The purpose of the Amendment Act was to bring Indian legislation in line with international norms, such as the United Nations Commission on International Trade legislation's (UNCITRAL) Model Law on Electronic Commerce[12].

Data Protection Provisions

Sections 43A and 72A, in particular, which form the foundation of India's present data protection law, were included as special data protection measures in the IT Amendment Act of 2008.

Section 43A of the Act[13].

Section 43A of the IT Act holds corporate entities (also known as 'body corporates') liable if they control, manage, or administer a computer resource that contains sensitive personal data or information (SPDI). They must create and keep 'reasonable security practises and procedures' in place to prevent unauthorised access, damage, disclosure, or other abuse of such information. A business body may be held accountable for paying the damaged party if it violates specific

[11] "What is the Information Technology Amendment Act 2008 (IT Act 2008)?, available at: https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008."
[12] "Shiv Shankar Singh, 'Privacy and Data Protection in India: A Critical Assessment' 53 *JILI* 663–77 (2011)."
[13] The Information Technology (Amendment) Act, 2008, s. 43A.

 [ISSN 2581-5369]

security practises and procedures, causing that person undue injury or gain.

In compliance with Section 43A of the IT Act, the Ministry of Electronics and IT (MeitY) has released the IT (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011." These criteria include the collection, storage, disclosure, and transfer of sensitive personal data or information, as well as the implementation of appropriate security policies and practises by organisations.

Section 72A.

Section 72A of the IT Act covers the problem of intermediaries or service providers disclosing personal information without permission. This clause punishes anybody, including an intermediary, who deliberately or intentionally divulges personal information received under a lawful contract without the agreement of the person in issue or in violation of the contract's conditions. Section 72A criminal penalties include a possible three-year prison term, a maximum five-lakh rupee fine, or both.

(B) The DPDP Bill, 2022

Data protection has become more important as the amount of personal information collected, processed, and stored on a global basis has increased. In light of its fast increasing digital economy, India has acknowledged the need to safeguard personal data and has built a comprehensive legislative framework to do so." It may use this framework to govern the acquisition, storage, processing, and transfer of personal data. The purpose of this research is to give a comprehensive examination of the DPDP Bill, 2022 ('DPDP Bill') and its implications for data security in India.

The DPDP Bill is a key piece of legislation that intends to build a strong data protection framework in India, protecting people' personal information and addressing privacy, security, and abuse of personal information issues. The following are the primary goals of the DPDP Bill:

- Ensure that personal data is handled in a secure and lawful manner in order to protect people's basic right to privacy.
- Create the India Data Protection Authority (DPAI) to oversee and enforce the country's data protection regulations.
- Provide people with particular rights and remedies to give them more control over their personal data.
- Hold data fiduciaries and processors accountable for adhering to data protection rules.

 [ISSN 2581-5369]

- Create protections for cross-border data transfers and allow free movement of personal data inside India.

Rights of Data Subjects

The DPDP Bill offers data principals several rights, providing people more control over their personal data. Among these rights are:

- Data subjects have the right to view their personal information and get confirmation that their information is being handled.
- Data controllers have the right to request the deletion of any personal information that is no longer required for the purposes for which it was obtained, as well as the correction of incorrect data.
- Data principals have the right to have their personal information transferred to another data fiduciary and accessed in a structured, widely used, and machine-readable format.
- Individuals have the right to object to the processing of their personal information, including for direct marketing reasons." [14]

Data Fiduciary and Data Processor Obligations

The DPDP Bill puts various requirements on data fiduciaries and data processors in order to guarantee that data protection principles are followed. These responsibilities include:

- To put privacy into practise from the start, data fiduciaries must include privacy into all of their operations, procedures, and systems.
- Data fiduciaries must assess the risks of processing personal data, especially when new technologies or large-scale processing are employed.
- A substantial data fiduciary must appoint a data protection officer who will be in responsible of managing data protection measures and ensuring compliance with the DPDP Bill.
- In the event of a personal data breach, data fiduciaries must immediately inform the DPAI and impacted data principals.
- Data fiduciaries must keep records of their data processing operations and be prepared to show compliance with the DPDP Bill upon request[15].

[14] "Shiv Shankar Singh, 'Privacy and Data Protection in India: A Critical Assessment' 53 *JILI* 663–77 (2011)."
[15] "Dr. Ajay Kumar Garg Ms. Shikha Kuchhal, 'Data Protection Laws in India: A Comparative Study,' 3 *IT* 75 (2013)."

 [ISSN 2581-5369]

(C) Data Protection Authority of India (DPAI)

The DPDP Bill establishes the Data Protection Authority of India (DPAI), a distinct regulatory organisation entrusted with carrying out and regulating the nation's data protection regulations. The DPAI's primary duties are as follows:

- encouraging stakeholders to understand and be careful of data protection.
- Monitoring and implementing the DPDP Bill, including audits and the imposition of fines.
- resolving disagreements between data fiduciaries and data principals.
- assisting the government on data protection issues.
- fostering engagement and international collaboration in data protection problems.

(D) Critique and Analysis

- **Strengths**

The DPDP Bill establishes a strong and comprehensive legislative framework for data protection in India, addressing issues such as data protection principles, data subjects' rights, data fiduciary and data processor requirements, and regulatory monitoring.

- The DPDP Bill is meant to improve cross-border data flows and build confidence in India's digital ecosystem, in accordance with international norms. It adheres to international data protection regulations such as the GDPR.
- Sensitive DPDP: The DPDP Bill includes special rules for sensitive DPDP, such as explicit authorisation requirements and strengthened security measures for processing such data.

The establishment of the DPAI, an independent regulatory organisation that would properly administer and supervise the country's data protection regulations, is one of the primary advantages of the DPDP Bill.

(E) Concerns and Limitations

- Overreliance on consent: The DPDP Bill's dependence on consent as the principal legal basis for processing personal data may provide commercial issues and may not always offer data subjects with meaningful alternatives.
- Businesses have expressed worry about the DPDP Bill's data localization measures, which they say would increase operating costs, impede cross-border data flows, and

 [ISSN 2581-5369]

possibly isolate India's digital economy.

- Lack of flexibility in cross-border data transfers: In comparison to the GDPR, the DPDP Bill's cross-border data transfer rules are stricter, which may present challenges for multinational enterprises and impede India's involvement in the global digital economy.
- The ability and resources of the DPAI to supervise and enforce India's data protection rules will be critical to the DPDP Bill's efficacy in practise. The DPAI will need enough budget, people, and training to properly administer the DPDP Bill.
- Balancing data protection with other policy goals: The DPDP Bill must find a compromise between preserving individual privacy rights and allowing legitimate data usage for economic, innovation, and general welfare progress. The present form of the bill has been criticised for putting data privacy ahead of other legislative goals.

IV. OVERLAPPING CONCERNS WITH IPR

The relationship between data security and IPR has grown in importance in the digital age. Although both domains have the same goal—protecting valuable assets and encouraging innovation—their scope and emphasis vary. This section investigates the link between IPR and data protection, specifically database protection.

- **Database Protection**

Databases are data collections that have been organised systematically for convenient retrieval, analysis, and management. They have grown into critical assets in the digital economy because firms depend on them for decision-making, research, and product creation. As a result, protecting databases from unauthorised use, access, or copying has become critical.

- **Sui Generis Database Rights**

i. Justification and conceptualization

Sui generis database rights are a kind of IP protection that is unique to databases. The goal of these rights is to protect database creators' significant time, effort, and financial commitment. Traditional intellectual property regulations, such as copyright law, may not be enough to safeguard databases since they put greater emphasis on the creative components of a work than on the effort required in acquiring or collecting the data[16].

[16] "Francesco Banterle, 'The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis,' 5 *PDCCPIPL* 411 (2018)."

 [ISSN 2581-5369]

ii. European Union (EU) Database Directive

The European Union (EU) realised the necessity for specific database rights and created them with the Database Directive (Directive 96/9/EC). The Directive currently gives database producers the exclusive ability to restrict the extraction and reuse of all or a portion of their databases. Security is given 15 years after the database is completed.

To be eligible for protection under the Directive, a database must demonstrate that acquiring, verifying, or displaying its contents necessitated a significant expenditure. The Directive also allows for the use of a combination of copyright and sui generis database rights to protect databases, as long as the database meets the standards for both types of protection.

iii. Possibility of Use in India

India presently lacks a specialised database protection system. Some databases, on the other hand, may be protected by the Copyright Act (1957) if they fulfil the standards for 'literary works' and demonstrate the required degree of originality and ingenuity. However, since it concentrates on the creative element of the work, this protection may not effectively address the investment made by database developers.

Given the rising significance of databases in the Indian economy and the limitations of the Copyright Act, it may be advantageous to build a specific database protection scheme in India. This would need a detailed examination of other nations' experiences, such as those of the EU, as well as a rigorous evaluation of the advantages and disadvantages[17].

India may stimulate the construction and expansion of databases, as well as innovation in data-reliant fields, by introducing sui generis database rights. Furthermore, it has the potential to improve India's status as a center for data-driven firms and aid the country's digital growth.

Adopting such a legislation, however, would present some difficulties. For example, it is critical to create a balance between the interests of database developers and the general public's interest in information access. Furthermore, defining the protected territory and determining what constitutes a 'substantial investment' or 'substantial part' at acceptable levels may be problematic.

(A) Copyright Protection for Databases

Due to the nature of databases and how their value frequently crosses the border between innovation and investment, database protection under copyright law has been a source of

[17] "Rachit Garg, 'Data privacy and intellectual property rights', *available at*: https://blog.ipleaders.in/data-privacy-intellectual-property-rights/ (Visited on April 05, 2023)."

substantial discussion and legal development. This section will go through the copyright protection available for databases, with a focus on the importance of creativity, compilation and selection criteria, and relevant Indian and international case law.

i. Authenticity Must Be Demonstrated

Original works of writing that have been permanently fixed in a physical medium are normally protected by copyright. "The desire for originality in the context of databases may be difficult to meet since databases often lack aesthetic or creative expression. Databases, on the other hand, may be eligible for copyright protection provided they utilise sufficient creativity in their data selection, coordination, or organisation.

In India, the Copyright Act of 1957 protects 'literary works,' which may incorporate databases provided the standards for originality are met. Although the Act does not define 'originality,' the Indian court has interpreted it to indicate that the work must be distinct and include a 'modicum of creativity' or intellectual effort.

ii. Criteria Selection and Compilation

If a database demonstrates originality or intellectual effort in the collection and selection of data, it may be protected as a literary work under the Copyright Act. This implies that the database author used judgement or expertise in selecting, arranging, or organising the data in a unique and original manner.

It is critical to emphasise that copyright protects only the selection, coordination, or arrangement of data, not the data itself. Individual data items included inside databases are consequently not protected by copyright since they are viewed as unprotected facts or ideas.

(B) RMI

RMI is information that identifies a work, its creator, the copyright owner, and any limitations on how it may be used. Metadata from digital content, such as the author's name, the title of the work, and copyright information, may be included in RMI. The primary goals of RMI are to make copyright administration and enforcement easier, as well as to allow the licencing, supervision, and distribution of copyrighted works in the digital world[18].

i. Privacy and Metadata Concerns

As metadata encoded in digital material may contain personal information about the author, copyright owner, or user of the work, the usage of RMI presents certain privacy issues.

[18] "Rights Management Information (RMI Definition), *available at*: https://www.lawinsider.com/dictionary/rights-management-information-rmi (Visited on April 08, 2023)."

 [ISSN 2581-5369]

According to data protection regulations such as the Indian DPDP Bill, 2022, personal data must be gathered, processed, and stored in accordance with the principles of lawfulness, fairness, and openness. When dealing with metadata containing personal information, companies managing RMI must ensure that they follow data protection regulations.

Additionally, monitoring user behaviour, such as preferences and consumption patterns, may be part of the collection and processing of RMI. Businesses must get the users' agreement before collecting and using their personal information in this context, according to data protection legislation.

ii. The Right to Forget and RMI

Under some conditions, people may be allowed to seek the erasure of their personal data from online sources under the right to be forgotten, a notion recognised under data protection legislation. This right may be in conflict with RMI when personal data about a person is contained in the metadata of a protected work.

Businesses that handle RMI must carefully balance the necessity to keep RMI for copyright enforcement with the right to be forgotten. They should consider whether the individual's right to privacy overrides such interests, or if continued processing of personal data in the RMI is required for the protection and enforcement of IPR.

(C) RMI and Copyright Law

i. Legal Protection for RMI in India

RMI is protected in India under Sections 65A and 65B of the Copyright Act, 1957. TPMs meant to safeguard intellectual property are forbidden under Section 65A, despite the fact that RMI is explicitly addressed in Section 65B. It is unlawful to distribute, import, or otherwise make accessible to the public any work or copy of a work in which the RMI has been removed or modified, according to Section 65B. It is also prohibited to remove or change any RMI without the owner's permission.

By penalising unauthorised manipulation of RMI connected with copyrighted works, these rules attempt to protect the integrity of RMI and prevent possible copyright infringement.

ii. Framework and Global Comparisons

RMI is also protected on a worldwide basis by a variety of treaties and agreements. Under the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), member states are expected to provide effective legal protection against the unauthorised removal or alteration of RMI. Furthermore, under the rules of the TRIPS , member nations are

 [ISSN 2581-5369]

expected to offer appropriate legal remedies in the instance of TPM circumvention and unlawful manipulation of RMI.

(D) The Role of Social Media in IPR and Data Protection

People's communication, information sharing, and content creation have all been altered by social media platforms. These platforms let users to create and share a broad range of material, including text, images, videos, music, and other creative creations. While social media platforms provide several advantages, they also pose issues in terms of data security and IPR .

User-generated content (UGC) on social media platforms may include works protected by copyright or other kinds of IPR . Furthermore, these platforms often capture massive quantities of user data, creating worries about user privacy and data security. It is so critical to strike a balance between encouraging innovation and creativity, maintaining IPR, and protecting user privacy.[19]

(E) Liability of Intermediaries

i. Safe Harbour Clauses

The IT Act of 2000 and the IT (Intermediaries Guidelines) Rules of 2011 are the two pieces of law in India that govern the liability of intermediaries. These provisions grant intermediaries a 'safe harbour' that shields them from liability for third-party content hosted on their platforms if certain requirements are met, such as exercising due diligence and promptly removing or disabling access to infringing content upon receiving actual knowledge of it or a court order.

As monitoring and pre-screening the large quantity of UGC uploaded on social networking sites would be almost impossible, safe harbour protections are critical for these firms. However, these restrictions raise issues regarding the efficiency of IPR enforcement and the possibility of intermediary misuse.

ii. Procedures for dispatch and takedown

The notice-and-takedown mechanism, which enables rightsholders to warn intermediaries of potentially infringing material and seek its removal, is a critical component of India's intermediary responsibility system. To retain their safe harbour status, intermediaries must delete or limit access to the material within 36 hours of receiving such notification.

While the notice-and-takedown approach provides intellectual property owners with a vital tool for preserving such rights, it has been criticised for being readily exploited, resulting in the

[19] "Michael Luca, 'User-Generated Content and Social Media', *available at*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549198 (Visited on April 08, 2023)."

removal of lawful material and restricting free expression. To address these issues, more open and equitable methods that protect the interests of both rights holders and users are required.

(F) Privacy and Copyright Concerns

i. Text and Data Mining

Data mining and text analysis algorithms are often used by social media platforms to analyse user-generated content (UGC) for a number of reasons, including targeted advertising, content suggestion, and sentiment analysis. While these practises may enhance user experiences, they also pose copyright and privacy problems since they may entail the use of personal data without the users' knowledge, as well as the unauthorised use of works protected by copyright.[20]

To address these challenges, rules and best practises for data mining and text analysis that respect users' privacy and IPR must be developed. This involves, for example, acquiring express agreement from users, using privacy-preserving techniques, and adhering to data protection standards and regulations.

ii. Content Ownership and User Confidentiality

The ownership and management of UGC is another key problem at the junction of IPR and data security on social media platforms. Many platforms' terms of service provide them extensive rights to use, copy, and distribute user-generated material, frequently without the users' express approval or understanding. Users' private rights are being abused, and there are concerns that their inventiveness will be exploited.

To solve these issues, it is critical to encourage openness in social media platform terms of service and to notify users of their duties and rights about their material. Politicians should also consider enacting legislation that respects and protects users' rights to their own material and requires platforms to get express agreement before utilising or distributing such data.

V. REGULATORY AUTHORITIES FOR DATA PROTECTION

(A) Central and State-level Authorities

In India, data security is overseen by a mix of national and state-level institutions. These entities play a critical role in ensuring that the statutory framework for data protection is successfully implemented and that data subjects' rights are safeguarded. This section will concentrate on the roles and obligations of India's major federal and state-level agencies concerned in data protection.

[20] Mireille Hildebrandt, '5. Privacy and Data Protection', 5 *LCS* (2019).

 [ISSN 2581-5369]

(B) Ministry of Electronics and IT (MeitY)

The Ministry of Electronics and IT (MeitY) in India is the central government entity in charge of developing and implementing projects and policies pertaining to electronics, IT, and general data security. MeitY's primary responsibilities include:

- Creating and enforcing laws, rules, and regulations to promote electronic governance, digital infrastructure, and data security.
- Collaborating with other federal, state, and international organisations and authorities to ensure that data protection laws and regulations are followed.
- Facilitating the growth of India's electronics and IT industries, including R&D, skill development, and general digital economy expansion.
- Monitoring the implementation and enforcement of the DPDP Bill after it is adopted in 2022.

(C) Central Bureau of Investigation

The Central Bureau of Investigation (CBI), India's principal investigative agency, handles high-profile cases including economic crimes, cybercrime, and corruption. The CBI's Cyber Crime Investigation Cell (CCIC) investigates data breaches, hacking, and other crimes involving the abuse of personal data. The CCIC collaborates closely with other law enforcement organisations in India and throughout the world to efficiently investigate and punish cybercriminals. The following are some of the CBI's major data protection responsibilities:

- Investigating situations of personal data abuse and data breaches in accordance with the IT Act of 2000 and other applicable regulations.
- Assisting and coordinating with other law enforcement authorities in cybercrime investigation and prosecution.
- Planning and implementing cybercrime prevention and response measures, such as public awareness campaigns, capacity development, and international collaboration.

(D) State-level Cyber Crime Cells

In addition to the federal authorities, each state in India has its own Cyber Crime Cell in charge of investigating and prosecuting cybercrimes, especially those concerning data security. State-level Cyber Crime Cells collaborate closely with the CBI and other central authorities to ensure that data protection rules are properly adhered to. The several state police agencies are in charge

 [ISSN 2581-5369]

of them. The following are the primary duties of state-level cybercrime cells:[21]

- Investigations and prosecutions for data breaches and personal data abuse in compliance with the IT Act of 2000 and other applicable state legislation.
- Working with the CBI and other federal, state, and local entities to ensure that data protection rules are rigorously followed.
- Providing technological help and support to other law enforcement bodies in their investigations and prosecutions of cybercrimes committed inside their respective countries.
- Developing and implementing state-level initiatives to prevent and fight cybercrime, such as public awareness campaigns, capacity development, and international collaboration.

VI. ROLE OF THE DATA PROTECTION AUTHORITY OF INDIA (DPAI)

Under the DPDP Bill, 2022 (DPDP Bill), the Data Protection Authority of India (DPAI) is envisioned as an independent regulatory authority. The DPAI will be critical in ensuring that India's data privacy rules are properly administered and enforced. Its primary tasks and talents are as follows:

- Monitoring and enforcing compliance with the DPDP Bill and other applicable data protection rules and regulations.
- Registration of data fiduciaries and data processors, as well as their grant, renewal, suspension, or cancellation.
- Complaints and suspected breaches of the DPDP Bill or other data protection laws and regulations are investigated.
- Imposing administrative fines and penalties for data protection regulations violations.
- Advising the federal government on data protection issues, including the development and implementation of standards, guidelines, and regulations.
- Improving data subjects', data fiduciaries', and data processors' comprehension of data protection requirements.
- Promoting international collaboration and engagement in data protection concerns such

[21] "Details about Indian Cybercrime Coordination Centre (I4c) Scheme, *available at*: https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme (Visited on March 15, 2023)."

 [ISSN 2581-5369]

as cross-border data transfers and mutual legal aid.

(A) Independence and Accountability

"The DPDP Bill emphasises the authority's independence from political or industrial involvement in order to maintain the authority's effectiveness in carrying out its functions. To choose members of the DPAI, the Bill proposes a selection committee comprised of specialists from the court, the executive branch, and academia. Political involvement in the employment process is reduced with this strategy.

In addition, the DPAI will be held responsible to both Parliament and the judicial system. Parliament must receive an annual report documenting the authority's actions, inquiries, and enforcement measures. Furthermore, there is an appellate tribunal to which DPAI rulings may be appealed, guaranteeing judicial control and a system of checks and balances.

(B) **Challenges and Opportunities**

The formation of the DPAI poses both obstacles and opportunity for India's data security environment. Among the most difficult problems are:

- Resource Constraints: As a newly constituted regulatory agency, the DPAI will need enough financial and personnel resources to carry out its responsibilities. The DPAI's efficacy is dependent on making these resources available, especially in a developing nation like India.
- Capacity Development: The DPAI must increase its technological expertise, legal understanding, and enforcement capabilities. Spending on acquiring, keeping, and educating competent individuals, as well as creating institutional competence, will be required.
- Privacy and Innovation: The DPAI must strike a careful balance between protecting people's privacy and supporting technological innovation. Overly rigorous regulations may impede innovation, while insufficient enforcement may jeopardise data subjects' rights."
- On the other side, the formation of the DPAI provides a number of possibilities for the Indian data protection ecosystem:
- Increased Compliance: The DPAI's supervision and enforcement skills will assist establish a stronger data protection system by encouraging data fiduciaries and data processors to comply.

 [ISSN 2581-5369]

- Increased Public confidence: A robust DPAI may aid in increasing public confidence in digital services and platforms, promoting increased adoption and involvement in India's digital economy.
- foreign Cooperation: As a specialised data protection authority, the DPAI can collaborate more effectively with foreign colleagues, fostering cross-border data flows and enabling reciprocal legal assistance in data protection concerns.

VII. SECTOR-SPECIFIC DATA PROTECTION REGULATIONS

Despite the fact that the DPDP Bill, 2022 (DPDP Bill) attempts to establish a comprehensive framework for data protection across all sectors, many organisations have unique needs and difficulties that necessitate sector-specific data protection regulations. This section will go through the major industry-specific data protection regulations and the institutions in charge of enforcing them in the financial, healthcare, and telecommunications industries.

(A) Financial Sector

Reserve Bank of India (RBI)

The Reserve Bank of India (RBI) is India's major financial regulator and central bank. It is in responsibility of safeguarding data security in the financial industry by issuing rules, circulars, and instructions to banks and non-banking financial corporations (NBFCs). The RBI has released a number of critical data security rules, including:[22]

- Master Direction on IT Framework for the Non-Bank Financial Institutions Sector: This legislation establishes the fundamental cybersecurity and IT governance requirements that NBFCs must adhere to in order to preserve the privacy, availability, and integrity of their clients' personal information.
- Master Directive on System Audit in Cooperative Banks (2018): "This directive requires cooperative banks to conduct system audits to assess the performance of their IT infrastructure, cybersecurity policies, and data protection practises.
- Payment System Data Storage (2018): According to this circular, all payment system providers must keep their payment system data in India, allowing for greater administration and control of sensitive financial data.

Securities and Exchange Board of India (SEBI)

[22] "Ankita Singh and Simran R. Grover, 'The Requirement of Sector-Specific Regulations in the Data Privacy Regime', *available at*: https://ijpiel.com/index.php/2021/12/24/the-requirement-of-sector-specific-regulations-in-the-data-privacy-regime/ (Visited on March 18, 2023)."

The Securities and Exchange Board of India (SEBI) is India's primary securities regulator. SEBI has issued a number of regulations and recommendations to protect sensitive data in the securities business, including:

- SEBI (Investment Advisers) Regulations for 2013: These regulations oblige investment advisors to follow data protection laws and keep customer information secret.
- Cyber Security and Cyber Resilience Framework (2015): This framework establishes essential cybersecurity and cyber resilience standards for stock exchanges, clearing bodies, and depositories, with a focus on securing sensitive market data.

(B) Ministry of Health and Family Welfare

The Ministry of Health and Family Welfare (MoHFW) is in charge of India's healthcare system. Despite the fact that there is no comprehensive regulatory framework for data privacy in the healthcare industry, the Ministry of Health and Family Welfare has issued guidelines and recommendations to safeguard sensitive health data, such as the Electronic Health Records (EHR) Standards for India (2016). These guidelines, with a focus on patient health information security, establish the essential standards for generating, maintaining, and transmitting electronic health records.

(C) Telemedicine Guidelines

In response to the Covid-19 outbreak, the MoHFW released Telemedicine Practise Guidelines in 2020. These rules provide requirements for preserving patients' privacy and health information during virtual consultations and give legal support for telemedicine in India". Data protection standards must be followed by health professionals who offer telemedicine services, such as gaining informed permission, preserving data confidentiality, and ensuring data security.

(D) Telecom Sector

Department of Telecommunications (DoT)

The Department of Telecommunications (DoT) regulates India's telecom industry. "The Department of Transportation has provided a number of ideas and rules to safeguard sensitive user data in the telecom industry, including:

- Contract for the Provision of Internet Services: This agreement requires Internet Service Providers (ISPs) to take necessary security procedures to secure customer data and ensure network traffic confidentiality.

 [ISSN 2581-5369]

- Guidelines for Telecom Service Providers (2011) on Data Protection, Data Security, and Privacy Telecom service providers must follow these rules to secure sensitive customer data. These rules establish the core data protection and security requirements.

Telecom Regulatory Authority of India (TRAI)

The Telecom Regulatory Authority of India (TRAI) is India's principal telecom regulatory organisation. The Telecom Regulatory Authority of India (TRAI) has set guidelines and rules to safeguard customer data and privacy in the telecom industry. Among the most important suggestions are:

i. 2018 telecoms industry suggestions on data privacy, security, and ownership These recommendations underline the significance of data protection and advocate for the development of a comprehensive legislative framework for data protection in the telecommunications industry. They also call for the formation of a Data Protection Authority to supervise the industry's adherence to data protection rules.

Draught Telecommunication Rules (Prepaid Payment Instrument Security) (2020): These draughts rules establish the security parameters for telecom prepaid payment devices such as mobile wallets and prepaid cards, with a focus on securing sensitive financial and personal data."

VIII. INTERSECTION WITH OTHER LEGAL FRAMEWORKS

(A) Right to Privacy under the Constitution

Justice K.S. Puttaswamy v. Union of India

A major case from 2017, Justice K.S. Puttaswamy v. Union of India[23], "had a profound influence on India's data protection environment. In this case, the Supreme Court's nine-judge panel unanimously decided that the right to privacy is a basic freedom guaranteed by Article 21 of the Constitution, which also protects the right to life and individual liberty.

The Court noted that the right to privacy involves both the protection of personal data and the privacy of information. The ruling emphasised the need of India having a comprehensive legal structure in place to safeguard people's privacy and personal information, paving the way for the drafting of the DPDP Bill, 2022.

(B) Implications for Data Protection Laws

The Puttaswamy decision has an impact on India's data protection regulations in a variety of

[23] AIR 2017 SC 4161.

ways. It starts by emphasising that the government is required under the constitution to ensure data protection. This implies that any future or current data protection law must be consistent with the constitutionally protected right to privacy.

Second, the judgement emphasises the necessity for need and proportionality when invading someone's privacy. Any data protection regulation must guarantee that personal information is only collected, utilised, and shared when necessary and for lawful reasons, therefore minimising the effect on privacy.

The Puttaswamy decision underlines the need of openness, accountability, and individual ownership over personal data. These rules, which are now part of India's data protection regulations, must be incorporated in every new law.

(C) Consumer Protection and E-commerce

Consumer Protection (E-Commerce) Rules, 2020

The Consumer Protection Act of 2019 established the Consumer Protection (E-Commerce) Rules, 2020 to protect consumers'" interests in the rapidly expanding e-commerce industry. These rules impose a number of requirements on e-commerce businesses, including the protection of customer data.[24]

The following important provisions of the Consumer Protection (E-Commerce) Rules relate to data protection laws:

- Rule 4(2): E-commerce businesses must inform customers about their items' return, refund, exchange, warranty, and guarantee, as well as the accepted payment methods, the security of those methods, and any penalties or fines that may apply. This provision informs customers of the security procedures in place to secure their personal and financial information.
- Rule 4(4) makes it illegal for e-commerce enterprises to disclose a customer's private information to a third party without the customer's express permission. This criterion is in accordance with data protection rules, such as purpose restriction and consent.
- Rule 5: In order to resolve customer concerns, each e-commerce business must establish a grievance redressal procedure and designate a grievance officer. The issues of privacy and data protection are addressed here.

[24] "Consumer Protection (E-Commerce) Rules, 2020, *available at*: https://consumeraffairs.nic.in/theconsumerprotection/consumer-protection-e-commerce-rules-2020 (Visited on March 19, 2023)."

 [ISSN 2581-5369]

(D) Intersection with Data Protection Laws

Consumer Protection (E-Commerce) Rules, 2020 and data protection laws sometimes interact. Both frameworks aim to defend users' digital rights, especially when it comes to personal information.

To begin, both the Consumer Privacy Rules and the data privacy legislation emphasise the importance of permission in the acquisition and use of personal data. Before collecting, using, or disclosing a customer's personal information, e-commerce businesses must get their express permission.

Second, both frameworks compel firms to inform customers about their data protection policies in an easy-to-understand way. This section provides information on the categories of personal data gathered, the purposes for which it is used, and the security measures in place to secure it.

Finally, both the Consumer Protection Rules and the data protection legislation emphasise openness, accountability, and dispute resolution mechanisms. To resolve client concerns, e-commerce enterprises must implement grievance redressal mechanisms and appoint grievance officers, particularly those pertaining to data security and privacy. This guarantees that customers may seek redress if their data privacy rights are breached.[25]

IX. CASE STUDIES FROM INDIA AND OTHER DEVELOPING COUNTRIES

A number of Indian and worldwide cases addressing the subject of database copyright protection have affected our understanding of the originality requirement, as well as the criteria for compilation and selection.

D.B. Modak v. Eastern Book Company[26] : The Supreme Court of India concluded in this key case that originality criteria for copyright protection involve some degree of creativity or intellectual labour beyond just 'sweat of the brow' or 'industrious collection.' The court further said that only the original components of a work would be protected by copyright, not the information included inside.

Rajnish Chibber v. Burlington Home Shopping Pvt. Ltd.[27] : In this case, the Delhi High Court found that if a database was created or arranged with creative effort," it might be protected as a literary work under copyright law. "The plaintiff's regularly organised and maintained client

[25] "Update Note on Consumer Protection (E-Commerce) Rules, 2020 – Legal Developments, *available at*: https://www.legal500.com/developments/thought-leadership/update-note-on-consumer-protection-e-commerce-rules-2020/ (Visited on March 20, 2023)."
[26] Appeal (civil) 6472 of 2004.
[27] 1995 IVAD Delhi 732.

 [ISSN 2581-5369]

database was found to be a copyrightable work by the court.

Rural Telephone Service Co. v. Feist Publications, Inc. [28]: This United States Supreme Court decision altered the way creativity is seen in respect to databases. The court ruled that a database could only be protected by copyright if its selection, coordination, or organisation demonstrated some degree of innovation, rejecting the 'sweat of the brow' approach. Furthermore, the court concluded that copyright does not apply to data and facts.

Danske Dagblades Forening v. Informationpaq International A/S [29]: In this judgement, the European Court of Justice (ECJ) set the originality requirements for copyright protection. According to the court, a work is regarded unique if it is the author's original intellectual production and demonstrates the author's individual style and creative judgements.

(A) Technological Protection Measures (TPMs)

TPMs (Technological Protection Measures) are critical for safeguarding and securing IPR, particularly in the digital domain. They also help to ensure the security and privacy of personal data, which is becoming more important in today's data-driven culture. This section will examine how TPMs relate to data protection and copyright law, with an emphasis on encryption, anonymization, digital rights management, privacy-enhancing technologies, anti-circumvention approaches, fair use, and key Indian and international cases.

i. Anonymization and encryption

Encryption and anonymization are TPMs that act to safeguard personal data from abuse, disclosure, and unauthorised access. Anonymization is the technique of deleting or changing personally identifiable information (PII) from a dataset in order to make identifying people difficult or impossible. The process of transforming data into a code to prevent unauthorised access is known as encryption." These strategies may assist businesses in complying with data protection regulations such as the DPDP Bill (2022) by protecting the privacy and security of personal data.[30]

ii. DRM (Digital Rights Management)

DRM is a collection of TPMs that regulate how copyrighted digital material is accessed, utilised, and distributed. Personal data may also be safeguarded with DRM technology by limiting access and use to certain persons or organisations. DRM systems, for example, might place restrictions

[28] 499 U.S. 340 (1991).
[29] [2009] ECR I-6569
[30] "Ekta Gupta and Prachi Srivastava, 'Technological Protection Measures in Copyright: A Critical Analysis of Virtual Piracy', *available at*: https://amity.edu/UserFiles/aibs/dd62Article-X%20(Page%2079-84).pdf (Visited on April 07, 2023)."

 [ISSN 2581-5369]

on access, require users to validate their identities, or limit the number of devices that can view a specific piece of material. DRM may therefore supplement data security measures by guaranteeing that personal data is only accessible or shared with permission and is only used for the specified purpose.

iii. **PETs, or privacy-enhancing technologies**,

Privacy-enhancing technologies (PETs) are a kind of TPM that tries to safeguard users' privacy and personal information. PETs may use data reduction, anonymization, pseudonymization, encryption, and other methods that minimise or eliminate the gathering, archiving, and processing of personally identifiable information (PII). Organisations that use PETs in combination with data protection regulations may lessen the likelihood of data breaches, identity theft, and other privacy violations.

(B) Interaction with Data Protection Law

Data protection rules and the preservation of trade secrets and sensitive information may occasionally clash when it comes to employee privacy rights, third-party disclosures, and data breach notifications.

i. Employees' Privacy Rights

Workers have a right to privacy when it comes to personal data, even if firms want to keep their trade secrets private. Data protection regulations, such as the DPDP Bill, 2022, require businesses to strike a balance between their own interests and the privacy rights of their employees in order to ensure that employee data collection, processing, and storage are lawful, equitable, and transparent.

ii. Disclosures by Third Parties

When organisations communicate sensitive information with other parties such as suppliers or business partners, data privacy rules may have an influence on the safeguarding of trade secrets. Enterprises must ensure that suitable measures, such as data sharing or data processing agreements, are in place in these scenarios to prevent unauthorised access to or disclosure of private information.

iii. Notifications of Data Breach

In the case of a data breach, data protection rules often require businesses to inform the appropriate authorities and impacted people. This commitment may collide with the company's requirement to safeguard the confidentiality of its trade secrets in certain instances. Businesses must use prudence to reduce the potential consequences of a data leak while keeping trade

 [ISSN 2581-5369]

secrets discreet to the greatest degree practicable.

X. BALANCING DATA PROTECTION AND IPR

(A) Public Interest and Exceptions

Finding a balance between DPDP and the encouragement of innovation and creativity is particularly difficult at the intersection of data protection and IPR . In the public interest, this balance must be achieved to guarantee that both data protection and intellectual property regimes serve social objectives while protecting individual rights.[31]

To meet public interest issues, IPR needs exceptions and constraints. "For example, under copyright law, the concept of 'fair use' allows for limited uses of copyrighted content without obtaining permission from the copyright owner, as long as such uses are for academic, investigative, journalistic, or critical purposes. The patent law framework, similar to compulsory licencing, allows the government to award a licence to a third party to use a patented innovation without the approval of the patent owners in situations when the public interest is at risk, such as during national emergencies or public health crises.

(B) Privacy and Confidentiality Concerns in IPR Enforcement

IPR enforcement efforts often include the gathering and processing of personal data, which raises issues about confidentiality and privacy. For example, in order to identify persons who are unlawfully sharing or utilising copyrighted content online, personal information such as IP addresses or browser histories may be required.

To address these issues, IPR enforcement tactics must be proportional and compatible with data privacy regulations. To strike the proper balance between IPR enforcement and data protection, take efforts such as obtaining court orders before accessing personal data or ensuring that data processing operations are clear and follow to data minimization requirements.

XI. CONCLUSION

IPR and data privacy are two themes that often intersect, creating a difficult quandary. Database protection, for example, may include both copyright and sui generis database rights, according to the EU Database Directive. Protecting trade secrets and sensitive information, on the other hand, necessitates the interaction of contract law, tort law, and data protection legislation. TPMs and RMI also demonstrate the junction of data protection and IPR, notably in the context of

[31] "Rafik Hamza and Hilmil Pradana, 'A Survey of Intellectual Property Rights Protection in Big Data Applications' 15 *Algorithms* 418 (2022)."

 [ISSN 2581-5369]

copyright law.

One of the issues created by the link between IPR and data protection is finding the optimal balance between conflicting rights and interests. Assuring, for example, that IPR enforcement does not jeopardise data protection rights or otherwise undermine the public interest. "Furthermore, for the legal protection of databases, TPMs, and RMI, a careful balance between the rights of producers and users, as well as between the protection of IPR and the promotion of information access, is essential. Significant Indian court decisions, such as the Academy of General Education, Manipal v. B. Malini Mallya , and Eastern Book Company v. D.B. Modak , show how courts have sought to resolve these difficult concerns.

India has a solid legal structure in place to protect many types of IPR, such as patents, copyrights, trademarks, designs, and geographical indications. The Patents Act of 1970, the Copyright Act of 1957, the Trade Marks Act of 1999, the Designs Act of 2000, and the Geographical Indications of Goods (Registration and Protection) Act of 1999 are the primary legislation controlling these rights. These laws, together with the enforcement instruments given by administrative and judicial organisations, seek to strike a balance between the rights holders' and the public's interests. India has also accepted a variety of international treaties and accords that govern the worldwide protection of IPR, such as the TRIPS Agreement, Berne Convention, Paris Convention, PCT, Madrid Protocol, WCT, and WPPT.

(A) Suggestions

Enactment of a Comprehensive Data Protection Law

Given the shortcomings of India's present data protection framework, it is critical to establish comprehensive data protection legislation that solves the current concerns generated by fast technology improvements and globalization. The DPDP Bill, 2019, should be passed as soon as possible to ensure that data privacy rights are appropriately respected while simultaneously supporting innovation and economic progress.

Recognition of Sui Generis Database Rights

To safeguard databases that do not match the originality standards for copyright protection, India may explore establishing sui generis database rights, comparable to the EU Database Directive. This would strengthen database security and motivate investment in database construction and maintenance with a balanced method that does not unnecessarily limit access to information.

 [ISSN 2581-5369]

Strengthening Trade Secret Protection

India should improve the legal protection of trade secrets and sensitive information by enacting specialised trade secrets legislation, which would give better clarity and uniformity in this area. Such laws should define the extent of trade secret protection, impose appropriate punishments for theft, and address the interdependence of trade secrets, data protection, and employee privacy rights".

Addressing the Challenges Posed by Technological Protection Measures (TPMs) and RMI

When developing copyright laws and regulations in India, politicians should carefully evaluate how TPMs and RMI effect data security, privacy, and information access. This includes ensuring that copyright exceptions and limits, such as fair use, are not undercut by TPMs and RMI, and that anti-circumvention measures in copyright law do not restrict legitimate uses of copyrighted works in an unreasonable manner.

Encouraging Collaboration and Dialogue

"To better understand the difficulties and possibilities at the intersection of these two sectors, stakeholders from the data protection and IPR domains should participate in open communication and cooperation. To encourage the sharing of ideas and the creation of best practises and policies that achieve the critical balance between data privacy and IPR, conferences, seminars, and other events may be held.

Enhancing Public Awareness and Education

If data privacy and IPR are to be properly secured and enforced, public comprehension and awareness of these concerns must improve. Professional training courses, focused educational initiatives, and the creation of resources and tools to assist people and organisations in navigating the intricacies of the legal frameworks that regulate IPR and data security might all help.

Finally, there are a variety of obstacles and possibilities connected to the interaction between data privacy and IPR that must be thoroughly researched and assessed. India can successfully navigate this complex landscape and ensure the robust protection of both data privacy and IPR by enacting comprehensive data protection legislation, recognising sui generis database rights, strengthening trade secret protection, addressing issues raised by TPMs and RMI, encouraging collaboration and dialogue, and improving public awareness and education".

*****

 [ISSN 2581-5369]

XII. REFERENCES

Legislations

- TRIPS
- Copyright Act, 1957
- Database Directive in the European Union (EU)
- IT Act, 2000
- Madrid Protocol
- DPDP Bill, 2019
- Trade Marks Act, 1999
- WIPO Copyright Treaty (WCT)
- WIPO Performances and Phonograms Treaty (WPPT)

Articles

- Bais, Y. 'Privacy and Data Protection in India: An Analysis,' 4 IJLMH (2021).
- Banterle, F. The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis, 5 PDCCPIPL 411 (2018).
- Garg, A. K. Kuchhal, S. 'Data Protection Laws in India: A Comparative Study,' 3 IT 75 (2013).
- George, M. P. 'A critical examination of the patent enforcement landscape in India,' 17 JILPLP 51 (2022).
- Hamza, R. and Pradana, H. 'A Survey of IPR Protection in Big Data Applications' 15 Algorithms 418 (2022).
- Hildebrandt, M. 'Privacy and Data Protection' 5 LCS 56 (2019).
- Kuner, C. 'The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards,' 33 NLRI 23 (2021).
- Montagnani, M. L. 'The Interface Between Intellectual Property and IT Law,' 5 HIPR 149 (2021).
- Patentable subject matter under Article 52(2) and (3) EPC: a whitelist of positive cases from the EPO Boards of Appeal—Part 1,' 13 JIPLP5 (2023).

 [ISSN 2581-5369]

- Singh, S. S. 'Privacy and Data Protection in India: A Critical Assessment,' 53 JILI 663–77 (2011).

*****

 [ISSN 2581-5369]