myresearchgo Volume 2, Issue 2, February 2026, ISSN: 3107-3816 (Online)

The Role of Intellectual Property Law in Governing Data Ownership

Barge Balaji Ramesh[1] Dr. Mannalal R. Pandiya[2] Dr. Sunil L. Lungare[3]

Research Scholar, Department of Law, Shri JJT University, Jhunjhunu, Rajasthan, India

Research Guide, Department of Law, Shri JJT University, Jhunjhunu, Rajasthan, India

Research Co-Guide, Department of Law, Shri JJT University, Jhunjhunu, Rajasthan, India

Abstract

This paper examines the role of intellectual property law in governing data ownership, analyzing how traditional IP regimes—such as copyright, patents, trade secrets, and database rights—apply to data in various forms. It highlights the challenges posed by the intangible, non-rivalrous, and dynamic nature of data, which often falls outside conventional ownership paradigms. The study further explores the limitations of existing legal frameworks in addressing issues of data access, sharing, and protection, particularly in contexts involving artificial intelligence, big data analytics, and cross-border data flows. Additionally, it evaluates emerging legal approaches and policy initiatives aimed at balancing innovation, economic interests, and individual rights, including privacy and data protection. The paper argues that while IP law plays a significant role in shaping data governance, it requires adaptation and integration with other legal regimes to effectively address contemporary challenges of data ownership in the digital age.

Keywords: Intellectual Property Law, Data Ownership, Copyright, Digital Economy, Data Governance, Legal Framework, Information Law, Data Protection

Introduction

The rapid expansion of the digital economy has brought data to the forefront as one of the most valuable assets of the modern era. From personal information shared on social media platforms to complex datasets generated by artificial intelligence and machine learning systems, data now underpins innovation, economic growth, and decision-making across industries. However, this rise in the significance of data has also raised critical legal questions regarding its ownership, control, and protection. Among the various legal frameworks that attempt to address these concerns, intellectual property (IP) law plays a pivotal role in shaping how data is governed, even though it was not originally designed with data ownership in mind.

Intellectual property law traditionally encompasses legal protections for creations of the mind, including copyrights, patents, trademarks, and trade secrets. These regimes are designed to incentivize creativity and innovation by granting exclusive rights to creators and inventors over their works. In the context of data, however, the application of IP law becomes complex and often ambiguous. Raw data, in its unprocessed form, is generally not protected under most IP regimes because it lacks the element of originality required for copyright protection. Nonetheless, databases, compilations, and structured datasets may qualify for protection if sufficient creativity or investment is involved in their selection, arrangement, or organization.

One of the central challenges in applying IP law to data ownership lies in distinguishing between ownership of data itself and ownership of the rights associated with its use. For instance, while a company may collect and store large volumes of user data, this does not necessarily grant it absolute ownership in the traditional sense. Instead, IP law may provide limited rights over how that data is compiled, processed, or commercially exploited. Additionally, other legal frameworks, such as data protection laws and contractual agreements, often intersect with IP law, further complicating the determination of data ownership.

Trade secret law has emerged as a particularly relevant branch of IP law in the context of data governance. Organizations frequently rely on trade secret protection to safeguard valuable datasets, algorithms, and analytics processes that provide a competitive advantage. Unlike other forms of IP, trade secrets do not require public disclosure, making them well-suited for protecting confidential business information, including proprietary data. However, this form of protection depends heavily on the implementation of reasonable measures to maintain secrecy, highlighting the importance of internal data governance practices.

Moreover, the global nature of data flows introduces additional complexities, as different jurisdictions adopt varying approaches to IP protection and data regulation. While some regions, such as the European Union, have introduced specific database rights, others rely more heavily on existing IP frameworks and contractual mechanisms. This lack of harmonization poses challenges for multinational corporations and raises concerns about enforcement, jurisdiction, and cross-border data transfers.

In this evolving landscape, intellectual property law continues to play a crucial, albeit imperfect, role in governing data ownership. As technological advancements outpace legal developments, there is an increasing need to reassess and adapt IP frameworks to better address the unique characteristics of data. Understanding the interplay between IP law and data ownership is therefore essential for policymakers, businesses, and legal scholars seeking to navigate the complexities of the digital age.

Understanding Data and Data Ownership

Data refers to raw facts, figures, or information that can be processed to generate insights. It can be categorized into personal data, non-personal data, proprietary data, and public data. Data ownership, in simple terms, refers to the legal rights and control over the collection, use, dissemination, and commercialization of data.

However, unlike physical property, data ownership is not always exclusive or absolute. Multiple stakeholders may have interests in the same dataset—for instance, a user who generates data, a company that collects it, and a third party that processes it. This multi-layered nature of data complicates the concept of ownership and necessitates legal mechanisms to define and enforce rights.

Limitations of Intellectual Property Law in Governing Data Ownership

Despite its importance, IP law has significant limitations when applied to data ownership:

1. **Lack of Direct Protection for Raw Data**

   Most IP regimes do not protect raw data or facts. This creates gaps in legal protection, especially for industries reliant on large datasets.

2. **Multiplicity of Stakeholders**

   IP law is not well-equipped to handle situations where multiple parties contribute to or have interests in the same data.

3. **Global Variations**

   IP laws differ across jurisdictions, making it difficult to establish consistent rules for data ownership in a globalized digital economy.

4. **Rapid Technological Change**

   Emerging technologies such as AI, the Internet of Things (IoT), and blockchain generate new forms of data that challenge existing IP frameworks.

5. **Public Interest Considerations**

   Excessive IP protection may hinder access to data, stifle innovation, and limit competition. Balancing private rights with public interest is a persistent challenge.

Interaction with Other Legal Frameworks

Because IP law alone cannot fully govern data ownership, it operates alongside other legal regimes:

1. **Data Protection and Privacy Laws**

   Laws such as the General Data Protection Regulation (GDPR) in the EU emphasize individual rights over personal data, including consent, access, and erasure. These laws focus on **control rather than ownership**.

2. **Contract Law**

   Contracts play a crucial role in defining data ownership and usage rights. Terms of service, licensing agreements, and data-sharing contracts often determine who can use data and under what conditions.

3. **Competition Law**

   Competition authorities may intervene when data concentration leads to monopolistic practices. Access to data can be a key factor in maintaining fair competition.

4. **Property Law Concepts**

Some scholars advocate for recognizing data as a form of property. However, this approach raises concerns about commodification and inequality.

Role of Data Protection Laws

Data protection laws are legal frameworks designed to safeguard personal information and ensure it is collected, processed, stored, and shared responsibly. In today's digital world, where vast amounts of data are generated and exchanged, these laws play a crucial role in maintaining trust, privacy, and security.

1. Protecting Individual Privacy

The primary role of data protection laws is to protect the privacy of individuals. They ensure that personal data—such as names, addresses, financial details, and online activity—is not misused or accessed without consent.

2. Regulating Data Collection and Use

These laws set rules on how organizations collect and process data. They require:

- Clear consent from users
- Purpose limitation (data used only for a specific reason)
- Data minimization (collect only necessary data)

3. Enhancing Data Security

Data protection laws mandate that organizations implement appropriate security measures (like encryption and secure storage) to prevent data breaches, hacking, or unauthorized access.

4. Granting Rights to Individuals

They empower individuals with rights such as:

- Right to access their data
- Right to correct inaccurate data
- Right to erase data ("right to be forgotten")
- Right to data portability

5. Promoting Accountability and Transparency

Organizations must be transparent about how they use data and are held accountable for misuse. Many laws require:

- Privacy policies
- Data protection officers
- Regular audits and compliance checks

6. Preventing Misuse and Cybercrime

By setting penalties and legal consequences, these laws deter misuse of personal data, identity theft, and cybercrimes.

7. Facilitating International Data Flow

Data protection laws create standards that help regulate cross-border data transfers, ensuring that data shared internationally remains protected.

8. Building Trust in the Digital Economy

When users know their data is protected, they are more likely to engage in online services like e-commerce, banking, and social media, supporting economic growth.

Challenges in Applying Intellectual Property Law to Data

The rapid growth of the digital economy has transformed data into one of the most valuable resources of the 21st century. Businesses, governments, and individuals generate and rely on vast amounts of data daily. However, the legal frameworks governing intellectual property (IP) were largely designed for traditional creations such as literary works, inventions, and artistic expressions. Applying these frameworks to data presents significant challenges due to the unique nature of data, its modes of creation, and its economic significance.

1. Nature of Data and Lack of Originality

One of the primary challenges in applying IP law to data lies in the nature of data itself. Intellectual property law, particularly copyright, protects works that demonstrate originality and creativity. However, raw data—such as facts, measurements, or statistics—is generally considered non-original and therefore not eligible for copyright protection. For example, a dataset containing temperature readings or financial figures does not involve creative expression. While a database may receive protection if it involves a creative selection or arrangement of data, the underlying data remains unprotected. This creates a gap where valuable datasets can be copied and reused without infringing copyright, reducing incentives for data collection and investment.

2. Difficulty in Defining Ownership

Data ownership is another complex issue. Unlike tangible property, data can be easily duplicated and shared among multiple parties simultaneously. This raises the question: who owns the data?

In many cases, multiple stakeholders contribute to data creation. For instance, user-generated data on digital platforms involves the user, the platform provider, and sometimes third-party service providers. Determining ownership rights among these parties becomes legally ambiguous. Traditional IP law does not adequately address such multi-layered ownership structures, leading to disputes and uncertainty.

3. Inadequacy of Existing IP Regimes

Existing IP regimes—copyright, patents, trademarks, and trade secrets—do not fully accommodate the characteristics of data:

- **Copyright** protects expression, not facts or data.
- **Patents** require novelty and inventiveness, which raw data typically lacks.

- **Trade secrets** can protect confidential data, but only as long as secrecy is maintained.
- **Database rights** (in some jurisdictions like the EU) offer limited protection but are not universally recognized.

This patchwork approach results in inconsistent protection across jurisdictions, making it difficult for organizations operating globally to safeguard their data assets.

4. Big Data and Aggregation Issues

The emergence of big data analytics further complicates IP protection. Large datasets are often created by aggregating data from multiple sources, some of which may be publicly available or owned by different entities.

This raises several challenges:

- Determining whether aggregated datasets qualify for IP protection.
- Identifying the rights of original data contributors.
- Addressing potential infringement when datasets are combined or transformed.

Additionally, the value of big data often lies in its volume and analysis rather than its individual components, making traditional IP frameworks less relevant.

5. Data Sharing vs. Protection

Modern economies increasingly rely on data sharing for innovation, particularly in sectors such as healthcare, artificial intelligence, and scientific research. However, strong IP protection may hinder data sharing, while weak protection may discourage investment.

Balancing these competing interests is a significant challenge. For example:

- Open data initiatives promote accessibility and transparency.
- Private companies seek to protect proprietary datasets for competitive advantage.

Striking the right balance between openness and exclusivity is difficult, especially when legal frameworks are not designed for such dynamic environments.

6. Cross-Border Issues and Jurisdictional Differences

Data flows seamlessly across borders, but IP laws are territorial in nature. Different countries have varying approaches to data protection and IP rights, leading to legal fragmentation.

For instance:

- The European Union provides database rights under the Database Directive.
- The United States relies more on contract law and trade secrets.
- Developing countries may lack comprehensive data protection laws.

These differences create uncertainty for multinational corporations and complicate enforcement of rights. Determining which jurisdiction's laws apply in cases of cross-border data disputes is often challenging.

7. Enforcement Difficulties

Even when legal protection exists, enforcing IP rights over data is problematic. Data can be copied, modified, and distributed instantly at minimal cost. Detecting infringement is difficult, especially when data is transformed or integrated into larger datasets.

Moreover, digital environments allow anonymous or pseudonymous use, making it harder to identify infringers. Legal proceedings can be costly and time-consuming, often outweighing the potential benefits of enforcement.

8. Role of Contracts and Technological Measures

Due to the limitations of IP law, organizations increasingly rely on contracts and technological measures to protect data. Licensing agreements, terms of service, and non-disclosure agreements are commonly used to regulate data use.

Technological tools such as encryption, access controls, and digital rights management (DRM) also play a role. However, these solutions have their own limitations:

- Contracts are only enforceable between parties who agree to them.
- Technological measures can be circumvented.
- Over-reliance on private arrangements may reduce transparency and fairness.

9. Ethical and Privacy Concerns

Data often includes personal information, raising ethical and privacy concerns that intersect with IP law. Granting exclusive rights over personal data can conflict with individuals' rights to privacy and control over their information. For example, companies that collect user data may claim proprietary rights, but individuals may object to how their data is used or monetized. Balancing IP protection with privacy rights is a complex legal and ethical challenge, especially under regulations like the General Data Protection Regulation (GDPR).

10. Emerging Technologies and Future Challenges

Technologies such as artificial intelligence (AI), machine learning, and the Internet of Things (IoT) are generating unprecedented amounts of data. These questions highlight the need for legal reform to address evolving technological realities.

Conclusion

In conclusion, intellectual property law plays a crucial but evolving role in governing data ownership in the modern digital landscape. While traditional IP frameworks—such as copyright, patents, and trade secrets—provide partial mechanisms for protecting certain forms of data, they were not originally designed to address the complexities of raw data, big data analytics, and digital information flows. As a result, gaps remain in clearly defining ownership rights, especially where data is non-rivalrous, collaboratively generated, or derived from users.

To remain effective, IP law must adapt to technological advancements and the growing importance of data as an economic asset. This includes balancing the interests of creators, businesses, and individuals while ensuring innovation, competition, and privacy are not compromised. Policymakers may need to develop new legal approaches or refine existing doctrines to better address issues such as data access, control, and fair use.

Ultimately, a coherent and forward-looking legal framework—integrating intellectual property principles with data protection and competition law—are essential to ensure that data is governed in a way that promotes innovation, protects rights, and supports equitable growth in the digital economy.

References

- Arezzo, E. G. (2019). Data ownership and data protection: Legal challenges in the digital economy. *European Intellectual Property Review, vol. 41*(6), page no. 345–353.
- Bently, L., Sherman, B., Gangjee, D., & Johnson, P. (2022). *Intellectual property law* (6th ed.). Oxford University Press.
- Burk, D. L. (2017). Owning e-science: Data ownership and data sharing in scientific research. *Minnesota Law Review, vol. 101*(5), page no. 1795–1852.
- Drexl, J. (2018). Designing competitive markets for industrial data. *Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 9*(4), page no. 257–292.
- Frischmann, B. M. (2012). *Infrastructure: The social value of shared resources*. Oxford University Press.
- Gervais, D. J. (2021). Exploring the interfaces between big data and intellectual property law. *Vanderbilt Journal of Entertainment & Technology Law, vol. 23*(4), page no. 713–745.
- Guibault, L., & Wiebe, A. (Eds.). (2013). *Safe to be open: Study on the protection of research data and recommendations for access and usage*. Göttingen University Press.
- Hugenholtz, P. B. (2017). Data property: Unwelcome guest in the house of IP. *European Intellectual Property Review, vol. 39*(3), page no. 147–152.
- Jentzsch, N. (2019). Data ownership in the age of big data. *International Data Privacy Law, vol. 9*(1), page no. 1–14.
- Lemley, M. A. (2015). IP in a world without scarcity. *New York University Law Review, vol. 90*(2), page no. 460–515.
- Meurer, M. J., & Bessen, J. (2008). *Patent failure: How judges, bureaucrats, and lawyers put innovators at risk*. Princeton University Press.
- Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review,vol. 57*(6), page no. 1701–1777.

- Purtova, N. (2018). The illusion of personal data as no one's property. *Law, Innovation and Technology, vol. 10*(2), page no. 245–267.
- Samuelson, P. (2000). Digital information, digital networks, and the public domain. *Law and Contemporary Problems, vol. 66*(1–2), page no. 137–171.
- Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review, vol. 86*(6), page no. 1814–1894.