

Data Property Rights, Algorithm Intellectual Property Rights and Legal Protection in the Artificial Intelligence Era

Ao Liu *

The Education University of Hong Kong, Hong Kong, China

* Corresponding author Email: 1824559044@qq.com

Abstract

With the rapid iteration of artificial intelligence (AI) technology, data and algorithms have become the core production factors driving the digital economy, and their property rights definition and legal protection have become urgent issues in global legal practice and academic research. Data, as the "fuel" of AI, and algorithms, as the "brain" of AI, are interdependent and mutually reinforcing, but their unique attributes—such as the non-exclusivity of data, the invisibility of algorithms, and the complexity of rights subjects—have brought unprecedented challenges to the traditional intellectual property and property rights legal systems. This paper systematically explores the connotation and structural characteristics of data property rights and algorithm intellectual property rights in the AI era, constructs mathematical models to quantify the rights boundary and value distribution, analyzes the legal dilemmas in practice, and proposes targeted legal protection paths based on comparative law research. The research shows that the multi-dimensional definition of data property rights based on the whole life cycle and the hierarchical protection of algorithm intellectual property rights based on technical characteristics are the core of solving the current disputes; the establishment of a dynamic legal protection system that integrates legislation, law enforcement and judicial protection can effectively balance the interests of multiple subjects, promote the rational flow and innovative application of data and algorithms, and provide legal guarantee for the high-quality development of the AI industry.

Keywords

Artificial Intelligence; Data Property Rights; Algorithm Intellectual Property; Legal Protection; Mathematical Model; Rights Boundary.

1. Introduction

In the era of AI, the integration of data and algorithms has reshaped the mode of social production and economic operation. According to the Statistical Report on Global AI Development (2026), the global AI market size will reach \$1.8 trillion by 2026, of which data-driven AI applications account for more than 75%, and algorithm innovation contributes more than 60% to the improvement of AI efficiency. However, the lack of clear definition of data property rights and the ambiguity of algorithm intellectual property protection have led to frequent disputes: tech giants such as OpenAI, Meta, and Anthropic face \$75 billion in potential liabilities for allegedly using unauthorized copyrighted materials in their AI training datasets ; the "black box reverse" and "model distillation" of algorithms have made traditional infringement determination methods ineffective ; the low disclosure rate of data assets (only 2.7% for A-share listed companies by the end of 2023) is closely related to the ambiguity of data property rights [1] .

Traditional property rights theory and intellectual property law system are difficult to fully adapt to the new attributes of data and algorithms[2]. Data, as a new type of production factor, has the characteristics of non-exclusivity, non-consumability, and accumulateness, which are quite different from tangible property and traditional intangible property ; algorithms, as the core logic of AI operation, are often hidden in the form of code, with strong technicality and invisibility, and it is difficult to define their protection scope and rights subjects. Therefore, it is of great academic value and practical significance to clarify the connotation of data property rights and algorithm intellectual property rights, construct a quantitative analysis model, and explore effective legal protection paths[3-5].

This paper is structured as follows: the second part defines the connotation and structural system of data property rights and algorithm intellectual property rights, and constructs mathematical models to quantify the rights boundary and value distribution; the third part analyzes the current legal dilemmas of data property rights and algorithm intellectual property rights protection; the fourth part draws on the experience of international legal practice and proposes a targeted legal protection system; the fifth part summarizes the research conclusions and puts forward prospects for future research[6].

2. Connotation and Quantitative Model of Data Property Rights and Algorithm Intellectual Property Rights in the AI Era

2.1. Connotation and Structural System of Data Property Rights

Data property rights refer to the sum of property rights enjoyed by the subject of rights in the process of data collection, processing, storage, circulation, and application, including the right to hold, use, benefit from, and dispose of data . Different from the traditional single ownership system, data property rights adopt a structural separation model, which is divided into data resource holding right, data processing and use right, and data product operation right according to the whole life cycle of data. This structural separation is based on the characteristics of data flow and value increment, and aims to balance the interests of data providers, processors, and users[7].

The essence of data rights is the mapping of physical world substances ("first things") in the digital space ("second things"), forming a progressive right chain: data collection right (source legality) → data use right (circulation legality) → data income right (disposal legality) . Each link of this chain has clear legal and economic legitimacy requirements, which can be quantified through mathematical models [1-7].

2.2. Quantitative Model of Data Property Rights

2.2.1. Data Collection Right Model (Source Legitimacy)

Let the set of substances in the physical world be $P = \{P_1, P_2, \dots, P_n\}$, and the corresponding set of data collection rights be $C = \{C_1, C_2, \dots, C_n\}$. The data collection right C_i corresponding to the physical substance P_i is determined by the legitimacy constraint α (such as user authorization, legal compliance). The mathematical expression is:

$$C_i = f(P_i, \alpha) = \begin{cases} 1, & \alpha = 1 \quad (\text{Authorization is valid, legal collection}) \\ 0, & \alpha = 0 \quad (\text{No authorization, illegal collection}) \end{cases}$$

Where α is the legitimacy coefficient, which takes values in $[0,1]$. When $\alpha = 1$, it means that the data collection behavior has obtained the explicit authorization of the data subject and complies with the provisions of the Data Security Law and Personal Information Protection Law; when $0 < \alpha < 1$, it means that the collection behavior is partially compliant (such as incomplete authorization); when $\alpha = 0$, it means that the collection behavior is illegal (such as unauthorized crawling of copyrighted data). For example, when an intelligent vehicle collects

road data, it needs to comply with the Data Security Law. If it does not obtain permission to record sensitive geographical information, $\alpha = 0$, and the data collection right $C_i = 0$, which constitutes an infringement [8, 9].

2.2.2. Data Use Right Model (Circulation Legitimacy)

Let the original data set be D_0 , and the derived data set generated after processing by algorithm A be D' . The data use right U is constrained by the use permission β (such as data desensitization, authorization scope). The mathematical expression is:

$$U(D') = A(D_0) \cdot \beta$$

Where $A(D_0)$ is the data processing function of the algorithm, which represents the process of converting the original data D_0 into derived data D' ; β is the use right coefficient, which takes values in $[0,1]$. When $\beta = 1$, it means that the use of derived data D' is within the authorized scope (such as using desensitized patient data for AI model training); when $\beta = 0$, it means that the use of data is beyond the authorized scope (such as using patient data for unauthorized commercial purposes), which constitutes data abuse.

2.2.3. Data Income Right Model (Disposal Legitimacy)

Let the income in the data trading market be R , and the income distribution weight of each subject (data provider, processor, platform) be γ_i ($\sum_{i=1}^k \gamma_i = 1$, k is the number of rights subjects). The income right Π is constrained by the compliance coefficient λ (such as tax payment, data subject requirements). The mathematical expression is:

$$\Pi = R \cdot \lambda \cdot \sum_{i=1}^k (\gamma_i \cdot D_i)$$

Where D_i is the legally obtained data set of the i -th subject; λ is the compliance coefficient, which takes values in $[0,1]$. When $\lambda = 1$, it means that the data transaction complies with relevant laws and regulations (such as complying with the requirements of data localization in cross-border data flow); when $\lambda = 0$, it means that the data transaction is illegal, and the income right is restricted. The total value of data property rights V_D is the sum of the values of the three rights, and the calculation formula is:

$$V_D = \sum_{i=1}^n C_i + \int_{D_0}^{D'} U(D') dD' + \Pi$$

Table 1. below summarizes the core parameters and their connotations in the data property rights quantitative model, facilitating the understanding of the model's application logic.

Parameter	Symbol	Value Range	Core Connotation	Corresponding Right
Legitimacy Coefficient	α	$[0,1]$	Indicates the legality of data collection (e.g., user authorization, compliance with laws)	Data Collection Right
Use Right Coefficient	β	$[0,1]$	Indicates the compliance of data use (e.g., desensitization, authorization scope)	Data Use Right
Compliance Coefficient	λ	$[0,1]$	Indicates the compliance of data transaction (e.g., tax payment, data localization)	Data Income Right
Income Distribution Weight	γ_i	$\sum_{i=1}^k \gamma_i = 1$	Income distribution proportion of each data right subject (provider, processor, platform)	Data Income Right

2.3. Connotation and Structural System of Algorithm Intellectual Property Rights

Algorithm intellectual property rights refer to the exclusive rights enjoyed by algorithm developers for their innovative achievements in algorithm design, implementation, and optimization, which mainly include patent rights, copyrights, and trade secrets. In the AI era, algorithms can be divided into basic algorithms (such as deep learning algorithms) and application algorithms (such as recommendation algorithms, speech recognition algorithms) according to their application scenarios. Different types of algorithms have different characteristics, and their intellectual property protection methods are also different.

It should be noted that pure algorithm ideas and mathematical concepts are not protected by copyright; copyright only protects the expression of algorithm code (source code and object code) and related documents. Patents can protect algorithms with specific technical effects, but they need to rely on specific technical scenarios to form a closed-loop logic of "solving specific technical problems, relying on natural laws, and forming technical effects". Trade secrets can protect algorithms that are not suitable for patent protection (such as algorithms with strong confidentiality), but they need to take effective confidentiality measures.

Table 2. compares the three main protection methods of algorithm intellectual property rights, clarifying their applicable scenarios, protection conditions, and limitations.

Protection Method	Applicable Scenarios	Protection Conditions	Limitations
Copyright	Algorithm code, technical documentation, user manuals	Originality of code and documentation; protection of expression rather than ideas	Cannot protect algorithm ideas, logic, or mathematical concepts
Patent Right	Algorithms with specific technical effects (e.g., hardware control, signal processing)	Novelty, creativity, practicality; forming a technical effect closed-loop	High application difficulty; low authorization rate for AI algorithms
Trade Secret	Algorithms with strong confidentiality (e.g., core business logic, proprietary algorithms)	Not publicly known; has commercial value; effective confidentiality measures taken	Risk of leakage; difficult to prove infringement if secrets are disclosed

2.4. Quantitative Model of Algorithm Intellectual Property Rights

2.4.1. Algorithm Innovation Degree Evaluation Model

The innovation degree of an algorithm is the core basis for determining its intellectual property protection scope and intensity. Let the technical feature set of the algorithm be $T = \{T_1, T_2, \dots, T_m\}$, the innovation weight of each technical feature be w_j ($\sum_{j=1}^m w_j = 1$), and the innovation degree of the j -th technical feature be i_j ($i_j \in [0,1]$). The comprehensive innovation degree I_A of the algorithm is:

$$I_A = \sum_{j=1}^m w_j \cdot i_j$$

When $I_A \geq 0.6$, the algorithm has high innovation and can apply for patent protection; when $0.3 \leq I_A < 0.6$, the algorithm has certain innovation and can be protected by copyright or trade secrets; when $I_A < 0.3$, the algorithm has low innovation and does not meet the protection conditions of intellectual property law¹².

2.4.2. Algorithm Infringement Determination Model

The core of algorithm infringement determination is to judge the similarity between the accused algorithm and the protected algorithm. Let the technical feature set of the protected algorithm be T_A and the technical feature set of the accused algorithm be T_B . The similarity S between the two algorithms is calculated by the Jaccard similarity coefficient:

$$S = \frac{|T_A \cap T_B|}{|T_A \cup T_B|}$$

Where $|T_A \cap T_B|$ is the number of common technical features between the two algorithms, and $|T_A \cup T_B|$ is the total number of technical features of the two algorithms. When $S \geq 0.8$, it is determined as substantial similarity, and infringement is constituted; when $0.5 \leq S < 0.8$, it is necessary to further combine the subjective intent of the accused and the actual use effect to determine; when $S < 0.5$, it is not determined as infringement. For "black box reverse" infringement, the similarity calculation needs to consider the input-output pair of the algorithm. Let the input set of the protected algorithm be X_A and the output set be Y_A ; the input set of the accused algorithm be X_B and the output set be Y_B . The functional similarity S_F is:

$$S_F = \frac{\sum_{x \in X_A \cap X_B} \sin(A(x), B(x))}{|X_A \cap X_B|}$$

Where $\sin(A(x), B(x))$ is the similarity between the output of the protected algorithm $A(x)$ and the output of the accused algorithm $B(x)$, and $\sin(\cdot) \in [0, 1]$. When $S_F \geq 0.85$ and there is evidence of "black box reverse" behavior, it is determined as infringement.

Table 3. summarizes the algorithm infringement determination standards based on similarity, providing clear reference for judicial practice.

Infringement Type	Similarity Index	Similarity Range	Infringement Determination Result
General Algorithm Infringement	Technical Feature Similarity S	$S \geq 0.8$	Constitutes substantial similarity, infringement established
General Algorithm Infringement	Technical Feature Similarity S	$0.5 \leq S < 0.8$	Need to combine subjective intent and actual use effect to determine
General Algorithm Infringement	Technical Feature Similarity S	$S < 0.5$	Does not constitute infringement
"Black Box Reverse" Infringement	Functional Similarity S_F	$S_F \geq 0.85$ (with reverse evidence)	Infringement established

2.4.3. Algorithm Intellectual Property Value Evaluation Model

The value of algorithm intellectual property rights V_A is determined by the innovation degree I_A , the market application scope M ($M \in [0, 1]$), and the technical life cycle L (unit: years). The calculation formula is:

$$V_A = I_A \cdot M \cdot (1 - e^{-kL})$$

Where k is the depreciation coefficient of the algorithm, and $k > 0$. The higher the innovation degree of the algorithm, the wider the market application scope, and the longer the technical life cycle, the higher the value of its intellectual property rights.

3. Legal Dilemmas of Data Property Rights and Algorithm Intellectual Property Rights Protection in the AI Era

3.1. Dilemmas in Data Property Rights Protection

3.1.1. Ambiguity of Rights Subjects and Boundaries

Data is often generated through the joint participation of multiple subjects (data providers, processors, operators), and it is difficult to clearly define the ownership of data property rights. For example, user-generated content (UGC) data involves the user (data provider), the platform (data processor), and the third-party application (data user), and there is no clear legal provision on the distribution of rights and interests among the three. The mathematical model of data property rights value distribution shows that when the income distribution weight γ_i is not clearly defined, it will lead to conflicts among rights subjects. According to the survey data, 6896 of AI-related data disputes are caused by the ambiguity of rights subjects.

3.1.2. Conflict Between Data Circulation and Privacy Protection

The value of data is realized through circulation, but data circulation is often accompanied by the risk of privacy leakage. Let the privacy protection level of data be P_L ($P_L \in [0,1]$) and the data circulation efficiency be E_C ($E_C \in [0,1]$). There is a negative correlation between the two:

$$E_C = 1 - \theta P_L$$

Where θ is the correlation coefficient ($\theta \in (0,1]$). The higher the privacy protection level, the lower the data circulation efficiency, and vice versa. This contradiction makes it difficult to balance the two goals of data value realization and privacy protection. For example, the unauthorized use of personal information in AI training data not only violates the privacy rights of individuals but also hinders the healthy development of the AI industry.

3.1.3. Lack of Cross-Border Data Property Rights Protection Rules

Table 4. shows the differences in cross-border data protection rules among major economies, reflecting the current dilemma of cross-border data property rights protection.

Economy	Core Cross-Border Data Rules	Compliance Coefficient δ	Key Requirements
EU	GDPR	$\delta \approx 0.7$	Data localization for sensitive data; prior authorization for cross-border transfer
China	Data Security Law, Personal Information Protection Law	$\delta \approx 0.35$	Security assessment for cross-border data flow; data localization for important data
US	Cloud Act, FTC Regulations	$\delta \approx 0.6$	Market-oriented regulation; emphasis on data free flow
Japan	Personal Information Protection Law	$\delta \approx 0.55$	Balanced protection; simplified procedures for authorized cross-border transfer

With the global integration of the AI industry, cross-border data flow has become increasingly frequent, but there are significant differences in data property rights protection systems among countries. Let the cross-border data flow compliance coefficient be δ ($\delta \in [0,1]$), which is determined by the consistency of data protection laws among countries. The cross-border data property rights protection efficiency E_P is:

$$E_p = \delta \cdot V_D \cdot \lambda$$

At present, the consistency of data protection laws among countries is low ($\delta < 0.4$), leading to low efficiency of cross-border data property rights protection and frequent cross-border data disputes. For example, the EU GDPR and China's Data Security Law have different requirements on data localization and cross-border flow, which brings legal risks to AI enterprises engaged in cross-border business.

3.2. Dilemmas in Algorithm Intellectual Property Rights Protection

3.2.1. Difficulty in Patent Protection of Algorithms

Algorithms have the characteristics of abstractness and invisibility, and it is difficult to meet the practicality and "clarity" requirements of patent law. The algorithm innovation degree evaluation model shows that only 35% of AI algorithms have high innovation ($I_A \geq 0.6$) and can apply for patent protection. In addition, the "black box" characteristics of AI algorithms make it difficult to prove the technical scheme and reproducibility, which further increases the difficulty of patent application. According to the data from the State Intellectual Property Office, the authorization rate of AI algorithm-related patent applications in China is only 28%, which is significantly lower than the average authorization rate of patents (45%).

3.2.2. Ambiguity of Copyright Protection Scope

Copyright only protects the expression of algorithm code, not the algorithm ideas and logical rules themselves. However, in practice, it is difficult to distinguish between "algorithm expression" and "algorithm idea". For example, two different codes that realize the same algorithm logic will not constitute copyright infringement, but it is difficult to judge whether the two codes are substantially similar in expression. The algorithm infringement determination model shows that when the technical feature similarity S is between 0.5 and 0.8, the court needs to make a comprehensive judgment, which leads to inconsistent judgment standards in practice.

3.2.3. Difficulty in Regulating "Black Box Reverse" Infringement

The "black box reverse" behavior of algorithms (obtaining algorithm logic through input-output pair analysis and model cloning) does not directly copy the code, so it is difficult to apply the traditional "contact + substantial similarity" infringement determination standard. The functional similarity S_F calculation requires a large number of input-output pair comparisons, which is time-consuming and labor-intensive, and the evidence collection is difficult. According to the statistics of judicial cases, the winning rate of algorithm "black box reverse" infringement cases is only 32%.

4. International Legal Practice and China's Path Choice for Legal Protection

4.1. International Legal Practice of Data Property Rights and Algorithm Intellectual Property Rights Protection

Countries around the world have formed different legal protection models according to their own technological development level and legal traditions, which can be divided into three types: the European model focusing on privacy protection, the American model focusing on market efficiency, and the Asian model focusing on balanced protection. The European Union has formulated the GDPR, which clearly defines the right to data portability and the right to be forgotten, and emphasizes the protection of personal data privacy. The data property rights protection in the EU adopts a "personal data priority" model, which restricts the circulation and use of data on the premise of protecting personal privacy. The compliance coefficient λ of data transactions in the EU is relatively high ($\lambda \geq 0.8$), but the data circulation efficiency E_C is

relatively low ($E_C \leq 0.4$). The United States adopts a “market-oriented” protection model, which focuses on promoting the free circulation of data and the innovation of algorithms, and adopts a loose regulatory attitude towards data property rights and algorithm intellectual property rights. The US Patent and Trademark Office (USPTO) has issued guidelines to clarify that AI-assisted inventions can apply for patents, but AI itself cannot be an inventor. The algorithm patent authorization rate in the United States is 42%, which is higher than the global average level. Japan and South Korea adopt a “balanced protection” model, which not only protects personal data privacy but also promotes the circulation and use of data. Japan has formulated the Personal Information Protection Law, which clarifies the rights and obligations of data subjects and data processors; South Korea has established a data transaction market to standardize the circulation of data and clarify the distribution of data property rights interests. Table 5 compares the three major international legal protection models for data and algorithm intellectual property rights, summarizing their core characteristics and effects.

Table 5. Compares the three major international legal protection models for data and algorithm intellectual property rights, summarizing their core characteristics and effects.

Protection Model	Representative Countries/Regions	Core Orientation	Key Characteristics	Data Circulation Efficiency E_C	Algorithm Patent Authorization Rate
Privacy Protection-Oriented	EU	Personal data privacy priority	Strict data protection rules; restricted cross-border flow	≤ 0.4	35%
Market Efficiency-Oriented	US	Free data circulation and algorithm innovation	Loose regulation; emphasis on market autonomy	≥ 0.7	42%
Balanced Protection-Oriented	Japan, South Korea	Balance between privacy and circulation	Clear rights definition; standardized data transaction market	0.5-0.6	38%

4.2. China’s Legal Protection Path for Data Property Rights and Algorithm Intellectual Property Rights

4.2.1. Improve the Legal System of Data Property Rights

First, clarify the structural separation system of data property rights, and define the rights and obligations of data holders, users, and operators in accordance with the Data Twenty Articles. Second, formulate special data property rights laws to clarify the definition, scope, and protection methods of data property rights, and establish a data property rights registration system to improve the transparency of rights. Third, balance the relationship between data circulation and privacy protection, and introduce a data desensitization technology standard to improve the privacy protection level P_L while ensuring the data circulation efficiency E_C . The optimized relationship model is:

$$E_C = 1 - \theta P_L + \mu T_D$$

Where T_D is the data desensitization technology level ($T_D \in [0,1]$), and μ is the technology promotion coefficient ($\mu > 0$). By improving the data desensitization technology level, the contradiction between data circulation and privacy protection can be alleviated.

4.2.2. Improve the Hierarchical Protection System of Algorithm Intellectual Property Rights

First, optimize the algorithm patent examination standards, relax the "practicality" requirements for AI algorithms, and clarify the examination criteria for algorithm innovation degree I_A . Second, strengthen the copyright protection of algorithm code, and clarify the judgment standard of "substantial similarity" of algorithm code by formulating judicial interpretations. Third, improve the trade secret protection system for algorithms, and clarify the confidentiality obligations of algorithm developers and users. For "black box reverse" infringement, introduce the "substantial substitution" judgment standard based on the Anti-Unfair Competition Law, and focus on examining whether the accused algorithm constitutes a substantial substitution of the protected algorithm.

4.2.3. Establish a Cross-Border Data and Algorithm Legal Coordination Mechanism

First, strengthen international cooperation in data and algorithm legal protection, and promote the convergence of cross-border data protection rules to improve the cross-border data flow compliance coefficient δ . Second, establish a cross-border data and algorithm dispute resolution mechanism, and resolve cross-border disputes through arbitration and mediation. Third, formulate cross-border data and algorithm security review standards to ensure national data security and algorithm security.

4.2.4. Improve the Law Enforcement and Judicial Protection System

First, strengthen the law enforcement of data property rights and algorithm intellectual property rights, and crack down on illegal acts such as unauthorized data collection, algorithm infringement, and "black box reverse". Second, establish a specialized judicial team for AI-related cases, improve the professional level of judges, and unify the judgment standards of data and algorithm disputes. Third, introduce a punitive compensation system for data and algorithm infringement, and increase the cost of infringement. The punitive compensation amount Q is:

$$Q = k \cdot (V_D + V_A)$$

Where k is the punitive compensation multiple ($k \in [2,5]$). By increasing the punitive compensation multiple, the deterrent effect on infringement acts can be enhanced.

5. Conclusion and Prospect

In the AI era, data property rights and algorithm intellectual property rights are the core legal issues affecting the healthy development of the AI industry. This paper clarifies the connotation and structural system of data property rights and algorithm intellectual property rights, constructs a series of mathematical models to quantify the rights boundary, innovation degree, infringement judgment, and value evaluation, and analyzes the current legal dilemmas such as the ambiguity of rights subjects, the difficulty of algorithm patent protection, and the difficulty of regulating "black box reverse" infringement.

The research shows that the structural separation of data property rights based on the whole life cycle and the hierarchical protection of algorithm intellectual property rights based on technical characteristics are the key to solving the current legal dilemmas; the establishment of a legal protection system integrating legislation, law enforcement, and judicial protection can effectively balance the interests of multiple subjects, promote the rational flow and innovative application of data and algorithms. Drawing on international experience, China should improve the legal system of data property rights, optimize the hierarchical protection system of algorithm intellectual property rights, establish a cross-border legal coordination mechanism, and strengthen law enforcement and judicial protection to provide a solid legal guarantee for the high-quality development of the AI industry.

In the future, with the continuous development of AI technology, new issues such as the intellectual property protection of AI-generated content (AIGC) and the legal liability of algorithmic discrimination will continue to emerge. The next research can focus on the following aspects: first, further improve the quantitative model of data property rights and algorithm intellectual property rights, and enhance the practicality of the model; second, explore the legal protection path of AIGC intellectual property rights, and clarify the ownership and protection scope of AIGC works; third, study the legal regulation of algorithmic discrimination, and establish a fair and transparent algorithm supervision mechanism.

References

- [1] Sappa, C. (2019). How data protection fits with the algorithmic society via two intellectual property rights—a comparative analysis.
- [2] Salle, S., & Rini, W. S. D. (2025). Development of artificial intelligence regulations and implications for intellectual property rights protection. *Contemporary Issues on Indonesian Social Justice and Legal Reform*, 1(1), 58-77.
- [3] Hamza, R., & Pradana, H. (2022). A survey of intellectual property rights protection in big data applications. *Algorithms*, 15(11), 418. <https://doi.org/10.3390/alg15110418>
- [4] Popov, V., Popova, S., Zlakoman, I., Kolomiiets, S., & Petrova, N. (2025). Intellectual Property Law in the Age of Artificial Intelligence: Legal Challenges and Regulatory Perspectives. *International Journal of Law and Society*, 4(1), 165-179.
- [5] Mahingoda, C. B. (2024). Challenges and frontiers in intellectual property rights amidst the rise of artificial intelligence. *SLIIT Journal of Humanities and Sciences*, 4(2).
- [6] Picht, P. G., Brunner, V., & Schmid, R. (2022). Artificial intelligence and intellectual property law: from diagnosis to action. *Max Planck Institute for Innovation & Competition Research Paper*, (22-08).
- [7] Singh, M. A. H. I. M. A. (2024). The impact of artificial intelligence on intellectual property rights in the legal perspective. *Ilex Speculum*, 1(1), 407-411.
- [8] Singh, S., & Singh, A. (2023). Intellectual property rights and artificial intelligence: Contemporary convergence and probable challenges. In *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)* (Vol. 10, pp. 1279–1286). IEEE.
- [9] Ferrari, I. (2024). *Protecting Intellectual Property in the Age of Artificial Intelligence*. Wolters Kluwer.