

GLOBAL GOVERNANCE STANDARDS

Article



DOI: 10.17803/2713-0533.2026.3.37.585-608

Legal Regimes Governing the Use of Prompts (Prompt Engineering) in the Training and Deployment of Large Language Models

Beniamin A. Shakhnazarov

Moscow Bar Association, Moscow, Russian Federation

© B.A. Shakhnazarov, 2026

Abstract: The paper examines the legal regimes governing the use of prompts in the training and deployment of large language models (LLMs) and generative artificial intelligence systems (AI systems). It analyzes risks, including prompt injection that may result in unauthorized access to information; intellectual property rights infringements, and AI systems manipulation. The paper further addresses the protection of prompts as objects of intellectual property, including protection under copyright law and trade secret regimes. Particular attention is devoted to jurisprudence in various jurisdictions, including China and the United States, where courts are developing approaches to determining the extent of human creative contribution in works generated with the assistance of AI. The study emphasizes the need for regulatory and technical measures to ensure security, oversight, and the allocation of responsibility in the use of generative AI systems.

Keywords: prompt engineering; large language models; prompt injection; artificial intelligence; intellectual property; copyright; trade secrets; AI safety; jurisprudence; liability

Cite as: Shakhnazarov, B.A., (2026). Legal Regimes Governing the Use of Prompts (Prompt Engineering) in the Training and Deployment

of Large Language Models. *Kutafin Law Review*, 13(3), pp. 585–608, doi: 10.17803/2713-0533.2026.3.37.585-608

Contents

I. Introduction	586
II. Literature Review and Methodology	587
III. Regulatory Background and Development of Approaches to Governing AI and Prompt Engineering	589
III.1. Security Governance of LLM Deployment: Prompt Injection as a Regulatory Policy Driver	590
III.2. Liability Models: from Policy Principles to Enforcement Concepts	593
III.3. Intellectual Property Governance in the Prompt – Model – Output Chain	595
IV. Law Enforcement	600
V. Conclusion	605
References	605

I. Introduction

In the modern world, the use of emerging information technologies in various spheres of human life has become an evident and indispensable element of the development of social relations. The acceleration, optimization, and increased efficiency of numerous processes, including cross-border interactions, have become possible through artificial intelligence systems (AI systems) capable of adaptively responding to a wide range of requests and tasks, processing and analyzing Big data, proposing effective solutions, and continuously learning, thereby improving information processing, feedback mechanisms, and responsiveness to users' needs.

Various states have adopted legal and regulatory instruments of differing legal force that, in one way or another, define policies and general principles governing the use and development of AI systems. Examples include the Decree of the President of the Russian Federation No. 490 dated 10 October 2019 (as amended on 15 February 2024) formally titled “On the Development of Artificial Intelligence in the Russian Federation” and approving the National Strategy for the De-

velopment of Artificial Intelligence through 2030;¹ on 8 July 2026, the State Duma of the Russian Federation adopted the Federal Law “On Supporting the Development of Artificial Intelligence Technologies in the Russian Federation” that permits the use of copyrighted works and related-rights-protected subject matter for the purpose of training national and sovereign large language models based on artificial intelligence (developed by Russian legal entities) without the consent of right holders and without payment of remuneration to them;² the Interim Measures for the Management of Generative AI Services of the People’s Republic of China (2023); the Executive Order of the President of the United States on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023);³ Regulation (EU) 2024/1689 on Artificial Intelligence (the EU Artificial Intelligence Act),⁴ etc.

Such regulatory activity of States at the national level demonstrates both the growing significance of AI systems and the risks associated with their use. At the same time, specific approaches to regulating particular aspects of AI technologies — including the legal status of prompts and prompt engineering as an intentional process of interacting with AI systems — have yet to be fully developed or clarified through legislation, judicial decisions, and administrative practice.

II. Literature Review and Methodology

Contemporary challenges arising from the use of prompts in training and deployment of large language models (LLMs), together with advances in artificial intelligence (AI) and the proliferation of AI-generated content, necessitate a forward-looking analysis and, in some re-

¹ Available at: <http://publication.pravo.gov.ru/Document/View/0001201910110003>. (In Russ.). [Accessed 11.07.2026].

² Draft Federal Law No. 1271570-8 “On Supporting the Development of Artificial Intelligence Technologies in the Russian Federation.” Available at: <https://sozd.duma.gov.ru/bill/1271570-8> [Accessed 13.07.2026].

³ Executive Order 14110 — Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. 30 Oct. 2023. Available at: <https://www.presidency.ucsb.edu/documents/executive-order-14110-safe-secure-and-trustworthy-development-and-use-artificial> [Accessed 11.07.2026].

⁴ Available at: <https://artificialintelligenceact.eu/> [Accessed 11.07.2026].

spects, a reassessment of earlier approaches, particularly approaches applied to protect intellectual outputs created with the assistance of such technologies. These developments also require the formulation of novel legal regimes governing the creation and use of intellectual outputs in the context of prompt engineering.

Given that prompt engineering in intellectual property area functions as an auxiliary instrument for the creation of intellectual outputs and, under current conditions of intellectual property regulation, should be harmoniously integrated into the relevant legal systems, this study employs general research methods including deduction and synthesis. In light of the heightened risks of infringement of intellectual property rights and circumvention of existing protection mechanisms associated with the use of prompts, the study also applies a comparative analytical method to assess prompt engineering in relation to existing legal regimes applied for the intellectual property protection.

Due to the legal character of this study, the author employs a formal legal method. Moreover, in light of the evolving nature of the relationships under examination and the emergence of divergent approaches in international practice, the study also adopts a comparative law methodology, analyzing the experiences of the Russian Federation, the People's Republic of China, and the United States.

Given the high degree of relevance and novelty of the legal relationships under consideration, as well as the lack of substantial judicial and administrative practice in this area, a considerable body of scholarly literature has already emerged addressing issues of prompt engineering and the protection of intellectual property rights in the use and training of LLMs. However, the scope and depth of research vary significantly across jurisdictions, which remains particularly important in light of the continuing application of territorial principle governing the protection of intellectual property rights. The majority of existing studies focus on issues of the protection and infringement of intellectual property rights in connection with the use of LLMs (Murray, 2024; Lee et al., 2022; Vyas et al., 2023; Aliyev, 2026; Ahuja, 2023).

Scholarly literature has already noted that recent cases in the United States and China underscore the significance of human involvement in the creation of AI-generated content, with courts closely examining

prompts, among other factors, in order to determine the extent of human contribution throughout the creative process (Lim, 2024). Scholars have also raised concerns regarding the risks associated with the reproduction of copyrighted materials in the context of generating individual works through prompts, particularly images (Reissinger et al., 2025). Specific risks arise from the use of AI diffusion models for image generation (Geiping et al., 2023), as well as from the development of AI-based solutions for the creation and operation of information services in the field of intellectual property (Lee, 2025). Collectively, these risks contribute to users' reluctance to make full use of the latest AI models (Reissinger et al., 2025).

Contemporary scholarship also devotes particular attention to issues of ownership arising from the use of artificial intelligence (Gaffar and Albarashdi, 2024; Jain and Verma, 2025). Comparative studies addressing the protection of intellectual property rights in AI-generated works have likewise been conducted (Burylo, 2022). Within the context of the present study, broader scholarship concerning the development of artificial intelligence is also of relevance. Such works highlight, in particular, that advances in artificial intelligence enable robots to learn and perform a wide range of practical tasks, which is expected to result in their widespread integration into contemporary society and interaction with the public, rather than solely within strictly controlled environments (Karnouskos, 2022). Particular attention should also be paid to studies examining the use of artificial intelligence, including the application of optimized prompts, for the detection and prevention of intellectual property rights infringements (Pokrovskaya, 2025).

III. Regulatory Background and Development of Approaches to Governing AI and Prompt Engineering

The potential interrelationship among different intellectual creations, as well as issues concerning the priority of exclusive rights, constitute significant challenges in the context of AI systems, since both insufficiently developed prompts and a high degree of AI autonomy — for example, where neural networks generate new intellectual property objects — may create risks of infringing the intellectual property rights

of third parties. Such infringements may occur not only with AI content generation, but also at earlier stages, namely, during large language models training, as well as through interaction with the AI system by altering instructions intended, among other things, to facilitate subsequent unlawful conduct.

III.1. Security Governance of LLM Deployment: Prompt Injection as a Regulatory Policy Driver

Prompt injection, namely, the insertion of malicious instructions into AI system inputs (Prompt Injection), constitutes one of the most pressing challenges facing contemporary generative artificial intelligence (GenAI) systems and large language models. This type of attack occurs when a person — or another AI system — induces a large language model to disregard or override its system instructions. The danger lies in the fact that such intentional actions may alter the functioning of informational and even physical infrastructure, while also infringing the rights and lawful interests of third parties.

The United Kingdom's National Cyber Security Centre has identified prompt injection as a critical risk, while the United States' National Institute of Standards and Technology has characterized this issue as the most significant security weakness of generative artificial intelligence (Sutton and Ruck, 2024). In the Open Worldwide Application Security Project statement, prompt injection occurs “when an attacker manipulates a large language model (LLM) through crafted inputs, causing the LLM to unknowingly execute the attacker's intentions.” Such attacks may result in the system's decision-making processes manipulation, dissemination of disinformation to users, confidential information disclosure, organization of sophisticated phishing attacks, and the malicious code execution.

The vulnerability associated with prompt injection arises when an attacker manipulates an LLM during prompting, that is, during the formulation of inputs or instructions for an AI system, through specially crafted input data that causes the model to unwittingly pursue the attacker's objectives.⁵

⁵ The OWASP Gen AI Security Project Official Website. LLM01: Prompt Injection. Available at: <https://genai.owasp.org/llmrisk2023-24/llm01-24-prompt-injection/> [Accessed 27.12.2025].

This may be accomplished either directly, through the “override” or compromise of system prompts, or indirectly, through manipulation of external input data, potentially resulting in data leakage, social engineering (including psychological manipulation of human behavior), and other harmful consequences.

A *direct injection* during prompting, also referred to as a “jail-break,” occurs when an attacker overrides or discloses the underlying system configuration, prompt, or instruction set. Such attacks may enable exploitation of vulnerabilities in backend systems by interacting with insecure functions and data repositories accessible through LLMs.

Indirect prompt injection is performed when an LLM accepts input from external sources that may be controlled by an attacker, such as websites or files. An attacker may embed malicious prompts into external content, thereby hijacking the conversation. This may undermine the stability and reliability of the model’s output control mechanisms, enabling the attacker either to manipulate the user or to compromise additional systems to which the LLM has access. Moreover, indirect prompts need not necessarily be visible or readable to humans; it is sufficient that the text be processed by the large language model itself.

It is important to recognize that the consequences of a successful direct injection attack may vary significantly, ranging from the confidential information disclosure to interference with critical decision-making processes disguised as ordinary system behavior.

As a result, the analytical, creative, project-management, and administrative functions of AI systems may lose their essential characteristics, namely, controllability and comprehensive moderation or administration by the user. Given the degree of trust users often place in outputs generated by LLMs, the user’s genuine expression of intent may effectively be compromised, thereby jeopardizing the potential benefits associated with the use of artificial intelligence.

Among the most common and illustrative vulnerabilities in generative AI systems are attacks in which a malicious actor employs a direct prompt injection instructing the LLM to disregard the developer’s system instructions and instead execute an unauthorized prompt intended to disclose confidential, dangerous, or otherwise undesirable information.

A user may also activate a plugin connected to an electronic marketplace. A malicious instruction embedded within a visited website may exploit such a plugin, resulting in unauthorized purchases, actions, or transactions. This problem has become widespread in part due to insufficient legal regulation in many jurisdictions concerning the allocation of liability in commercial activities carried out through online marketplaces.

Although no reliable protection against prompt injection into data streams currently exists for LLMs, a number of measures are already being implemented to counter such abuses and attacks and to mitigate their consequences. For example, when privileged operations are involved, e.g., sending or deleting emails, applications may be configured to require prior user confirmation before executing the action. This reduces the likelihood of unauthorized actions being carried out without the user's knowledge or consent through indirect prompt injection.

Another important safeguard involves establishing clear trust boundaries among the model, external data sources, and extended functionalities such as plugins or downstream functions. In this context, the large language model itself may be treated as an untrusted actor, while ultimate control over decision-making processes remains with the human operator or system administrator, including through the visual identification and labeling of potentially unreliable responses for end users.

The risks associated with generative AI systems may also arise through the insertion of malicious scripts into LLM-based support chatbots, including commands such as “ignore all previous instructions,” which may subsequently result in remote code execution, unauthorized access, and privilege escalation.

It is also important to consider the possibility of manipulation not only through information obtained from open Internet sources, emails, or messages, but also through documents that play a critical role in providing contextual information for RAG+LLM systems,⁶ particularly within large organizations. The use of documents in conjunction with

⁶ Retrieval-Augmented Generation systems that supplement user queries with information from external data sources.

LLMs creates a broad range of opportunities for prompt injection attacks, since such documents often contain substantially more information than ordinary emails and are frequently shared among groups of users through cloud-based document repositories such as *SharePoint* and *Google Drive* (Sutton and Ruck, 2024).

Attempts to manipulate AI systems, particularly LLMs, may and should be addressed within an appropriate legal framework. Where unlawful conduct carried out through prompting or prompt engineering infringes protected rights or interests, appropriate forms of responsibility should apply, ranging from civil liability to administrative and criminal sanctions.

III.2. Liability Models: From Policy Principles to Enforcement Concepts

A legal framework governing unlawful conduct involving AI systems should be based on two principles: technological traceability of the prompt manipulator, i.e., the offender who uses prompting techniques in connection with LLMs, and the inevitability of liability the determination and enforcement of which must account for the specific characteristics and capabilities of information technologies. In other words, the development of technologies, information systems, or generative AI systems within which it is impossible to identify or trace the offender and the offender's actions should be regarded as impermissible and unlawful. Accordingly, appropriate oversight and corresponding responsibility on the part of all relevant actors — from developers and administrators to users and consumers of AI-generated content — must be incorporated at every stage of the development and operation of AI systems.

The introduction of a presumption of culpable conduct on the part of the user of an AI system once an offense committed using large language models has been detected can constitute one more possible mechanism for balancing competing interests in this area.

Technical and informational measures aimed at preventing potential offenses in this sphere represent an important direction in the development of AI systems. Their implementation may operate within

both ethical and legal frameworks. Ethical guidelines, in particular, may and should play a distinct role in establishing principles governing the use of AI systems, serving as an initial regulatory mechanism.

For example, in order to reduce the risk of indirect prompt injection and related malicious activity, organizations should maintain appropriate data hygiene practices, assess systems prior to deployment, provide user training, and implement technical safeguards. Each of these strategies plays an important role in ensuring the security and resilience of generative artificial intelligence tools (Sutton and Ruck, 2024).

Before deploying a particular AI-based service, it is advisable to conduct a compliance assessment involving an analysis of internal and external information processes and information security risks, which is critically important for the subsequent scaling and integration of the relevant system. Such compliance procedures may themselves be automated. These activities may form part of a broader information security policy that takes into account the vulnerabilities of AI systems and the ongoing attempts undertaken by malicious actors to exploit malicious code and prompt injection techniques.

For the purposes of such compliance assessments, organizations should utilize continuously updated databases of indirect prompt injection strategies involving various document formats (including, for example, .doc, .pdf, and .png files), concealment techniques (such as hidden text in Word documents or white text on a white background), and attack vectors (including externally sourced email communications and direct access to document repositories in insider-threat scenarios).

At the same time, technical tools designed to counter such attacks, as well as automated compliance procedures, appear to require human oversight and expert moderation of automated compliance systems, given the rapidly evolving nature of threats in this field. With respect to the legal regulation of the relationships under consideration, these issues remain the subject of ongoing debate across multiple jurisdictions. In the United States, a comprehensive policy framework governing artificial intelligence remains limited, while data governance continues to depend largely on private industry and judicial litigation (Furqan et al., 2026). For example, most cybercrimes at the federal level are governed

by 18 U.S.C. § 1030, the Computer Fraud and Abuse Act (CFAA), which, inter alia, criminalizes unauthorized access to a computer or access exceeding authorization, i.e., the unlawful intrusion into an information system (Kilovaty, 2024).

Under 18 U.S.C. § 1030(a)(2), any person who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains... information from any protected computer” commits a criminal offense. Despite longstanding criticism of the CFAA, including concerns regarding its vagueness, overly broad scope, and outdated approach to computer intrusion, it has been argued that the AI systems manipulation may constitute unauthorized access and, accordingly, give rise to criminal liability.

This approach is based on the premise that circumventing a coded restriction through prompt injection constitutes a form of unauthorized access. In *Van Buren v. United States*,⁷ the U.S. Supreme Court articulated a criterion distinguishing authorized accesses from unauthorized access within an information system. According to the Court, the decisive criterion is the existence of a technological barrier preventing a user from accessing a particular part of a computer system. The Court referred to this approach as the “gates-up-or-down inquiry.” Although this analogy is not without limitations, its reasoning is grounded in a code-based conception of authorization. In essence, the relevant inquiry is whether technological code or a technical restriction that prevents a user from performing a specific action or accessing certain data exists,

Indeed, the circumvention of technical barriers, limits, or permissible boundaries governing the use of AI systems should reasonably be characterized as unlawful conduct where the rights of third parties are infringed, which is the case in most instances involving intentional acts.

III.3. Intellectual Property Governance in the Prompt — Model — Output Chain

Another significant issue associated with the use of GenAI systems concerns the protection of intellectual property rights in AI-related relationships.

⁷ *Van Buren v. United States*, 593 US 374 (2021). Available at: <https://www.oyez.org/cases/2020/19-783> [Accessed 11.07.2026].

This issue is not new to legal doctrine. Legal systems have generally addressed, both through legislation and judicial practice, the protection of intellectual property created either with the assistance of or autonomously by AI systems. Such approaches are typically grounded in the principle that only a human being may qualify as an author and copyright holder, while also recognizing, in many cases that AI-assisted outputs may constitute protectable intellectual creations where the applicable criteria for copyrightability or other forms of legal protection are satisfied and appropriately interpreted.

At the same time, it is necessary to distinguish the separate issue of the legal characterization and protection of prompts used for the effective operation of LLMs, including whether such prompts may qualify as copyrightable works or as know-how or trade secrets. Globally, there has been a growing practice of creating and systematizing prompts for use with particular generative AI applications, including the development of so-called “prompt libraries,” that, in certain circumstances, may themselves be eligible for copyright protection..

A prompt, as an instruction or query directed to an LLM, differs fundamentally from an ordinary search query. It may constitute an original creative input containing a role, contextual framework, task description, references to sources, and specifications regarding the format of the desired output. In essence, the creation and refinement of a prompt shapes and determines the resulting output.

It has been observed that the increasing frequency and intensity with which companies worldwide employ AI in their internal operations and commercial products has led them to rely more heavily on carefully designed instructions and effective prompts in order to improve the performance and outputs of AI systems.⁸ Such instructions may constitute valuable intellectual property and may be protected either under trade secret regimes or as copyrightable works. Businesses should treat them accordingly, taking into account both their commercial value and their creative character. This concerns the desirability of securing rights in prompts both within commercial operations and more broadly

⁸ Intellectual property protection for AI prompts. Intellectual Property, IP Agreements. *ShiftLaw*, 18 November 2025. Available at: <https://shiftlaw.ca/intellectual-property-protection-for-ai-prompts/> [Accessed 30.12.2025].

where a creative approach is employed in utilizing the capabilities of a particular AI system.

The operation of LLMs is impossible without prompts. A prompt may be simple or highly sophisticated. Not all prompts are necessarily eligible for copyright protection. However, as the desired result becomes more complex, the instructions required to achieve it likewise become more sophisticated. The development of effective prompts capable of optimizing AI performance may require substantial intellectual effort, numerous refinements and iterations, and extensive analytical reasoning. For example, marketers may use carefully engineered prompts to create unique content-generation instructions describing the characteristics of a particular brand; software developers may design prompts capable of generating optimized code fragments; and designers may employ prompts to produce distinctive visual styles.

Trade secret and confidential information law provides one of the most practical forms of protection for prompts. A trade secret is generally understood as information that derives economic value from not being generally known and with respect to which reasonable measures have been taken to preserve secrecy. This concept may logically encompass sophisticated instructions for generative AI systems or collections of such instructions, including AI prompt libraries developed internally by a company and used to improve internal processes or client services.

Prompts used for effective interaction with AI systems may qualify as copyright-protected literary “works” where they are treated as the result of the author’s creative effort and their creation required purposeful intellectual and analytical activity aimed at obtaining a particular result, including through multiple iterations of interaction with an AI system. It is important to recognize, however, that the content of a prompt cannot be determined solely by the desired outcome. In this respect, the situation is analogous to computer software source code that may be denied copyright protection where it constitutes the only possible means of achieving a particular function. Therefore, a copyrightable prompt differs from a simple search query intended merely to retrieve particular information.

This also raises issues concerning employee-created intellectual property. Where an employee uses generative AI systems and achieves

a unique result through the use of a unique prompt, copyright in the prompt itself may arise and may belong either to the employer or to the employee, depending on the applicable legal regime and on factors such as whether the prompt was created within the scope of the employee's duties or outside those duties.

The distinctive feature of copyright protection for AI prompts lies in the fact that copyright protects the form of expression of ideas rather than the ideas themselves. Consequently, infringement of copyright in a sophisticated AI prompt may potentially be avoided simply by expressing the underlying idea in different words. Where the idea itself possesses independent value, copyright may therefore not constitute an adequate mechanism of protection. In such cases, protection may instead be pursued through confidentiality regimes, trade secret law, or the protection of proprietary know-how, depending on the requirements of the legal system of the relevant jurisdiction.

Accordingly, for purposes of protecting prompts — particularly in commercial settings — companies using sophisticated AI prompts in analytical, creative, or other professional activities should develop and implement internal IP and AI policies, while also revising contractual arrangements with counterparties to ensure that unique AI prompts are treated as protected intellectual property assets and safeguarded against unfair competition. Recommended measures include maintaining the confidentiality of valuable AI prompts through access-control mechanisms and non-disclosure agreements (NDAs); documenting the economic value of proprietary prompts through independent valuation; clearly defining ownership of exclusive rights in prompts in agreements with independent contractors, vendors, and service providers; incorporating intellectual property provisions into terms of service governing AI tools; and registering or depositing copyrights in AI prompts with collective rights management organizations where applicable.

At the same time, organizations actively integrating AI-driven processes should consider how prompts and related materials fit within the company's broader intellectual property strategy.

Indeed, as the complexity of tasks assigned to artificial intelligence systems increases, or where greater specificity of output is required, prompts themselves must become more precise and sophisticated. As

a result, organizations increasingly rely on prompt engineers or even specialized prompt libraries or repositories, demonstrating the growing economic value attributed to these unique methods of task formulation and the steadily increasing market demand for them (Arnaiz Medina, 2024).

The protection of works under intellectual property law requires the existence of a literary, artistic, or scientific work that is original in the sense that it constitutes the author's own intellectual creation and represents an objective expression of the author's creative efforts. In this context, it is important to recognize that it is difficult to substantiate claims regarding the creative character or even the originality of a simple command where the command itself is not unique in its form, which is relatively uncommon. It may even be argued that a prompt closely resembles a description of an idea or a listing of elements sought in the final output rather than the work itself.

Nevertheless, there are areas of law — most notably computer software — in which these requirements have been interpreted more broadly. In the 1990s, as the commercial value of software became increasingly evident, copyright protection was extended to source code, including at the international level through the provisions of the 1994 TRIPS Agreement.

This development required a significant conceptual shift, namely the recognition that, in exceptional circumstances, works characterized less by artistic or creative value than by their utility or functionality may nevertheless qualify for copyright protection. The same logic may also be applied to prompts (Arnaiz Medina, 2024).

At the same time, prompts used to simplify interfaces and facilitate user interaction with AI systems frequently employ textual structures containing specific elements such as role, context, objectives, sources, and output format. The use of textual expression in prompts, where accompanied by creative effort and intellectual contribution on the part of the author, brings them conceptually closer to literary works, a category that, for purposes of legal protection, also encompasses computer software. Nevertheless, it is difficult to deny that the effectiveness, functionality, completeness, relevance, and uniqueness of the outputs generated through a given prompt constitute core characteristics of the

prompt itself and should be taken into account when assessing its eligibility for copyright protection.

In this context, it is also relevant to recall the distinctive nature of copyright protection afforded to databases, which were incorporated into the category of protected works based on criteria extending beyond originality alone, including the economic and human effort invested in their creation. Against this background, it cannot be excluded that certain sophisticated prompts may receive a degree of copyright protection, potentially including forms of limited, derivative, or *sui generis* protection.

Another important aspect of prompt protection concerns rights in content generated using prompts in generative AI systems. In such cases, the prompt itself may embody the creative character of the resulting work, and in that sense may constitute an integral component of the creative process protected by copyright law.

IV. Law Enforcement

Judicial practice worldwide is increasingly evolving toward the recognition of authorship in AI-assisted works where sufficient human creativity is demonstrated through the creation and refinement of prompts.

For example, in November 2023, the Beijing Internet Court in *Li v. Liu*⁹ held that the user was the author of an AI-generated image entitled “Spring Breeze Brings Tenderness” produced through the user’s moderation and prompting activities. In that case, the Court established that the author had entered approximately 30 prompts and more than 120 instructions in order to shape the generated image. The Court held that the image possessed the requisite originality, deriving this finding from the degree of contribution and effort demonstrated by the prompt author.

At the same time, international judicial and administrative practice reflects alternative approaches to the protection of works generated with the assistance of artificial intelligence. One example is the deci-

⁹ Beijing Internet Court Civil Judgment (2023) Jing 0491 Min Chu No. 11279. Available at: <https://english.bjinternetcourt.gov.cn/pdf/BeijingInternetCourtCivil-Judgment112792023.pdf> [Accessed 11.07.2026].

sion of the United States Copyright Office (USCO) — the government authority within the Library of Congress responsible for copyright registration and recordation in the United States — in the matter of *Zarya of the Dawn*.¹⁰ In that decision, the USCO acknowledged that prompts might influence the generated image, but do not directly and unequivocally determine a specific result, which remains inherently unpredictable. Particularly significant was the Office's conclusion that because the same prompt may produce different results on different occasions, the process necessarily involves an element of randomness in the operation of the AI system, making it impossible to conclude that the resulting work was created solely by the user.

In this regard, the direct causal relationship between the actions of the AI system user — expressed through the drafting and refinement of a particular prompt — and the resulting work, whose copyrightability must ultimately be assessed, appears to constitute one of the key factors in determining the existence of sufficient human creative contribution in the production of a work through technological means.

The USCO has previously denied copyright protection for several works generated using generative AI systems on the ground that they lacked sufficient “human creativity,” that is, sufficient creative contribution by a human author. However, by 2025 the Office appeared to adopt a more nuanced position when it granted registration for an AI-assisted work entitled “A Single Piece of American Cheese” created by graphic artist Kent Keirse. ¹¹ Although Keirse used *InvokeAI* in the creation process, the USCO concluded that the requisite human creativity was present through the author's selection, coordination, and arrangement of AI-generated content (Stephens, 2025).

Thus, traditional approaches to assessing the copyrightability of protected works, determining the author's creative contribution, and evaluating the resulting intellectual creation may also be applied to works generated with the assistance of artificial intelligence. At the

¹⁰ U.S. Copyright Office. *Zarya of the Dawn* (Registration # VAU001480196) (2023). Available at: <https://copyright.gov/docs/zarya-of-the-dawn.pdf> [Accessed 11.07.2026].

¹¹ Public Records System. VAU001543942 / 2024-08-05. Available at: <https://publicrecords.copyright.gov/detailed-record/37990563> [Accessed 11.07.2026].

same time, AI-assisted creation presents distinctive features, particularly in light of the high degree of autonomy characteristic of such technologies and the unique outputs generated by neural networks. In this context, it is critically important to determine the role of the individual involved in the creation of the work, the nature and extent of that person's creative contribution, and the degree of randomness in the resulting output and its relevance to the user's query.

Within this framework, particular significance attaches to the assessment of the prompt itself, including both its substantive dimension, i.e., its external textual form of expression, and its technical and functional characteristics, considered together with the operational logic of the specific AI system involved and the establishment of a direct relationship between the prompt and the resulting output.

At the same time, many aspects of these legal relationships remain unsettled at the current stage of AI development and deployment. Although China has recently been at the forefront of an approach recognizing that human control over AI tools used in content creation may justify copyright protection, a more recent case has introduced a degree of uncertainty into this position. In 2025, a court in Jiangsu Province dismissed a copyright infringement claim brought by a designer against a company that had manufactured children's plastic chairs without authorization based on designs created by the designer with the assistance of artificial intelligence (Stephens, 2025).

Designer Feng Runjuan created three chair designs using the AI service *Midjourney* and posted them on social media together with the prompt she had used. Her prompt read: "A children's chair with a jelly-like texture, shaped like a cute pink butterfly with a glass texture, against a light background." A chair manufacturing company approached Feng to license her designs, but the parties were unable to reach an agreement. Nevertheless, without authorization, the company proceeded to manufacture chairs bearing a resemblance to Feng's original designs by using her original prompt with certain modifications. Feng subsequently filed a lawsuit.

There was little doubt that the manufacturer had relied upon Feng's prompts in creating the chair design. However, the central legal issue

was whether the AI-generated designs could be regarded as original works eligible for copyright protection.

Feng was unable to reproduce the original images using the same prompts because of the stochastic and non-deterministic nature of the AI system. This circumstance led the court to conclude that the relevant design decisions had been made by the AI program rather than by the human who formulated the prompts. According to the court, the user was required to demonstrate a verifiable creative process involving the adjustment, selection, and refinement of generated images through additional instructions and parameter modifications, as well as deliberate and individualized choices reflecting substantial intellectual contribution to such visual elements as layout, proportions, perspective, arrangement, color, and lines composition.

The Court dismissed the case arguing that the disputed images did not satisfy the criteria for original works and therefore were not entitled to copyright protection.

Accordingly, depending on the specific factual circumstances of a case, courts — even within the same jurisdiction — may reach different conclusions. This reflects the continuing development of judicial approaches to intellectual property disputes involving AI-assisted creation and underscores the need to consider the technical and factual circumstances surrounding the generation of the intellectual output, including the role and extent of human participation in the creation of the work. Assessment of these factors is further complicated by the autonomous operation of AI systems and the potential infringement of third-party rights during content generation, circumstances that may not always be readily identifiable.

Indeed, the distinction between the Chinese cases discussed above largely rests on differing assessments of the degree of human involvement in the creation of both the prompts and the final outputs, although in Feng's chair-design case the court attached particular significance to the fact that the original images could not be reproduced using the same prompt.

As is well established, identical prompts frequently generate different outputs because of the operational characteristics of autonomous AI systems, which, in itself, does not indicate bad faith on the part of

the user. Nevertheless, the degree of human control and participation in the creation of the work remains a decisive factor, as demonstrated by decisions of courts and administrative authorities in both China and the United States — jurisdictions possessing some of the world’s most advanced AI ecosystems. With respect to the differing Chinese decisions discussed above, both may reasonably be regarded as carefully reasoned and well-founded, helping to establish criteria for distinguishing between works merely assisted by AI and works generated predominantly or entirely through autonomous AI processes.

Another important issue arising in connection with prompt engineering concerns liability for the infringement of third-party intellectual property rights. In China, for example, the so-called “Ultraman” case involved a judgment of the Guangzhou Internet Court, later affirmed on appeal by the Hangzhou Intermediate People’s Court, imposing liability for copyright infringement on a company that provided AI-powered text and image generation services through its website.¹²

The claimant was the Chinese licensee of a Japanese company holding rights to the well-known fictional character “Ultraman.” When users prompted the defendant’s AI image-generation system to create Ultraman-related content, the system generated images substantially similar to the copyrighted character covered by the claimant’s license agreement. The Court was required to determine whether the defendant had infringed the claimant’s rights of reproduction and adaptation and, if so, what remedies should apply.

Significantly, the Court held that although the defendant had not directly infringed the licensee’s rights, its failure to exercise reasonable care to prevent infringement — such as by warning users or implementing adequate filtering and blocking mechanisms — rendered it liable for contributory copyright infringement. The Court ordered the defendant to pay damages for 10,000 yuan, substantially lower than the 300,000 yuan sought by the claimant.

¹² Second Instance Civil Judgment in the Copyright Infringement and Unfair Competition Dispute between Shanghai Xinmou Cultural Development Co., Ltd. and Hangzhou Shuimou Intelligent Technology Co., Ltd. Available at: <https://www.ip-house.cn/casotypical/detail/1qdgw5827okrj334wgvj39ex4zvpnm.html> (In Chinese) [Accessed 11.07.2026].

The decision may be characterized as both sophisticated and well-reasoned, and it represents one of the earliest judicial decisions worldwide recognizing the potential liability of an AI platform for contributory copyright infringement (Stephens, 2025).

V. Conclusion

Legal relationships arising from the use of artificial intelligence in the creation of intellectual property objects may be characterized as complex, multi-layered, and technologically sophisticated. Their effective regulation requires careful determination of the role, degree of creative contribution, and level of control exercised over the technology, as well as the allocation of responsibility among individuals and other legal actors involved in the creation of intellectual outputs. The degree of creative contribution, the nature of human control, and both the direct and implied relationships among the actions of the human author, the developer of the AI system, and the user of the technology should form the basis for the parameterization of legal relationships concerning the protection and enforcement of intellectual property rights. These factors should serve as foundational criteria in identifying infringing parties and determining the nature and scope of violations of third-party rights arising from the use of artificial intelligence systems.

References

Ahuja, V., (2023). Artificial Intelligence and Copyright Issues and Challenges. *ILI Law Review*. Winter Issue, pp. 270–285. Available at: https://www.researchgate.net/publication/372418545_ARTIFICIAL_INTELLIGENCE_AND_COPYRIGHT_ISSUES_AND_CHALLENGES [Accessed 13.07.2026].

Aliyev, A., (2026). Legal Perspectives on the Legal Regulation of Ai-Generated Works and Issues on Legal Subjectivity of Artificial Intelligence. *Irpin Legal Journal*, pp. 155–163, doi: 10.33244/2617-4154-3(20)-2025-155-163.

Arnaiz Medina, V., (2024). Intellectual property and prompts: how to protect people who ask machines questions? Available at: <https://>

ponsip.com/en/ip-news/news/intellectual-property-and-prompts-how-to-protect-people-who-ask-machines-questions/ [Accessed 30.12.2025].

Burylo, Y., (2022). AI Generated Works and Copyright Protection. *Entrepreneurship Economy and Law*, 7–13. DOI: 10.32849/2663-5313/2022.3.01. Available at: https://www.researchgate.net/publication/362257085_AI_GENERATED_WORKS_AND_COPYRIGHT_PROTECTION [Accessed 13.07.2026].

Furqan, T., Aleissae, H.M., Ghenimi, N. et al., (2026). Global laws governing intellectual property rights for AI-generated works. *Discover Artificial Intelligence*, 6, article No. 449. Available at: <https://link.springer.com/article/10.1007/s44163-026-01165-8#citeas> [Accessed 13.07.2026].

Gaffar, H. and Albarashdi, S., (2024). Copyright Protection for AI-Generated Works: Exploring Originality and Ownership in a Digital Landscape. *Asian Journal of International Law*, 15(1), pp. 23–46, doi: 10.1017/S2044251323000735.

Geiping, J., Goldblum, M., Goldstein, T., Singla, V. and Somepalli, G., (2023). Understanding and Mitigating Copying in Diffusion Models. *arXiv:2305.20086*, pp. 47783–47803, doi: 10.48550/arXiv.2305.20086.

Jain, V. and Verma, R., (2025). AI and IP: Rethinking Ownership, Creativity and Rights. *International Journal for Multidisciplinary Research*, 7(2), doi: 10.36948/ijfmr.2025.v07i02.42466.

Karnouskos, S., (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, 30. Available at: https://www.researchgate.net/publication/351562821_Symbiosis_with_artificial_intelligence_via_the_prism_of_law_robots_and_society [Accessed 13.07.2026].

Kilovaty, I., (2024). When Manipulating AI Is a Crime. *LawFare*, 15 May. Available at: <https://www.lawfaremedia.org/article/when-manipulating-ai-is-a-crime> [Accessed 30.12.2025].

Lee, J., Le, T., Chen, J. and Lee, D., (2022). Do Language Models Plagiarize? Pre-print. Available at: https://www.researchgate.net/publication/359254924_Do_Language_Models_Plagiarize [Accessed 13.07.2026].

Lee, S., (2025). From Deep Learning to Vertical AI: Opportunities and Risks of Developing AI Solutions in the Intellectual Property Information Service. *Academy of Entrepreneurship*, 6, pp. 177–196, doi: 10.22815/JES.2025.6.2.177.

Lim, N., (2024). Prompting: What to know and does it matter for Intellectual Property? China, Malaysia, USA. *Lexology*, August. Available at: <https://www.lexology.com/library/detail.aspx?g=fa617cdf-641d-4d79-a329-b0a576b0b267> [Accessed 13.07.2026].

Murray, M., (2024). Generative AI Art: Copyright Infringement and Fair Use. *SMU Science and Technology Law Review*. 2024. 26. 259. Available at: https://www.researchgate.net/publication/377168438_Generative_AI_Art_Copyright_Infringement_and_Fair_Use [Accessed 13.07.2026].

Pokrovskaya, A., (2025). AI in Detecting and Preventing IP Infringements. *Erasmus Law Review*, 17, pp. 60–72. Available at: https://www.researchgate.net/publication/390850787_AI_in_Detecting_and_Preventing_IP_Infringements [Accessed 13.07.2026].

Reissinger, L., Li, Y., Haensch, A.-C. and Sarna, N., (2025). Safer Prompts: Reducing IP Risk in Visual Generative AI. Available at: https://www.researchgate.net/publication/391492961_Safer_Prompts_Reducing_IP_Risk_in_Visual_Generative_AI [Accessed 13.07.2026].

Stephens, H., (2025). Copyright Litigation in China: Some Interesting AI-Related Decisions from Chinese Courts. Available at: <https://hughstephensblog.net/tag/li-v-liu/#:~:text=In%20the%20prominent%20Li%20v,through%20a%20series%20of%20prompts> [Accessed 31.01.2025].

Sutton, M. and Ruck, D., (2024). Indirect Prompt Injection: Generative AI's Greatest Security Flaw Expert Analysis. Available at: <https://cetas.turing.ac.uk/publications/indirect-prompt-injection-generative-ais-greatest-security-flaw> [Accessed 28.12.2025].

Vyas, N., Kakade, S. and Barak, B., (2023). Provable Copyright Protection for Generative Models. Available at: https://www.researchgate.net/publication/368688377_Provable_Copyright_Protection_for_Generative_Models [Accessed 13.07.2026].

Information about the Author

Beniamin A. Shakhnazarov, Dr. Sci. (Law), Advocate, Moscow Bar Association, Moscow, Russian Federation

ben_raf@mail.ru

ORCID: 0000-0001-6968-0372

Received 18.01.2026

Revised 30.01.2026

Accepted 05.02.2026