Future Strategies for Digital Intellectual Property Protection

Mohamed FARAOUN*
Public Services and Development Laboratory
Djillali LIABES University, Sidi Bel Abbes, Algeria,
Mohamed.faraoun@univ-sba.dz

Date of submission: 06/04/2026 - Date of acceptance: 26/05/2026 - Date of publication: 27/07/2026

Abstract: The future strategy for Intellectual Property (IP) protection is shifting from traditional reactive legal frameworks to a proactive, "Code is Law" technical approach. This strategy centers on embedding digital defense mechanisms directly into creative works, such as "Data Poisoning" techniques to deter unauthorized scraping by AI algorithms. Furthermore, it leverages Blockchain technology as a decentralized ledger to verify creative authorship and "Smart Contracts" to automate royalty distribution and enforcement without intermediaries. This technical shift is complemented by emerging regulations mandating "Algorithmic Transparency" and the mandatory watermarking of AI-generated content. Ultimately, these strategies aim to establish a sustainable balance that safeguards human creative incentives while distinguishing between authentic human ingenuity and hybrid machine-generated outputs in a borderless digital landscape

Keywords: Artificial Intelligence, Blockchain, Data Poisoning, Smart Contracts, Digital Originality, Intellectual Property.

*** Corresponding author: Mohamed FARAOUN**

Introduction:

Today, the global intellectual property system faces a historic turning point, unprecedented since the **Berne Convention**. While the efforts of past decades focused on combating traditional **"digital piracy"**—represented by the unauthorized copying and distribution of works—the emergence of **Generative AI** has shifted the challenge from "content theft" to the "theft of creativity itself."

The transition from primitive piracy to **algorithmic modeling** raises complex issues regarding the nature of the author's **exclusive rights**. Machines are now capable of analyzing millions of protected data points and reshaping them into new forms that appear "original" at first glance, threatening to undermine the economic incentives for human creators. In this context, traditional laws, despite their flexibility, are no longer sufficient to govern this technological flux, as the pace of innovation far outstrips the speed of legislation.

We are facing a reality that demands a redefinition of **"Originality"** and **"Authorship,"** and a shift from a logic of punitive protection to one of **proactive protection** based on technology itself. The same Artificial Intelligence that threatens intellectual property could be the tool to protect it through **digital fingerprinting** and **smart contracts**.

This presentation seeks to diagnose this existential struggle between man and machine within the halls of patent and copyright offices. It envisions a future where thought is protected not only by rigid legal texts but by encrypted technical protocols that guarantee the creator's rights in a borderless digital world. Ultimately, it aims to establish a delicate balance between the free flow of information and the creator's right to protect the fruits of their intellectual labor from digital dissipation.

The Problem Statement Based on the above, we pose the following problem: **"How can the contemporary intellectual property system shift from being 'reactive' to digital piracy to being 'proactive' in facing the challenges of Artificial Intelligence? And what are the technical and legal mechanisms capable of protecting creators' rights without stifling technological innovation?"**

Section I: The Inadequacy of Traditional Rules Against "Algorithmic Piracy"

Section I: The Inadequacy of Traditional Rules Against "Algorithmic Piracy"

Piracy is no longer a simple act of "copying"; it has evolved into a process of **"cognitive appropriation"** carried out by Large Language Models (LLMs).

First: The Dilemma of Text and Data Mining (TDM)

AI companies rely on **Data Scraping** from the internet without prior authorization, classifying it as **"Fair Use,"** while creators view it as organized theft[1].

- **Definition of TDM in the Context of Intellectual Property:** Text and Data Mining (TDM) is defined as a technical process of extracting patterns and information from massive datasets of protected works (texts, images, music) to train AI models. The legal dilemma lies in the fact that this process requires making **"temporary copies"** or **"technical**

[1] Dr. Abdel Hadi Fawzi, *Intellectual Property in the Era of Big Data: A Comparative Study*, Dar Al-Fikr Al-Qanuni, Cairo, 2024, p. 45.

reproductions" of the works on corporate servers. This directly conflicts with the author's **exclusive right** to prevent the reproduction of their work without prior consent[2].

- **The Conflict Between "Fair Use" and "Commercial Exploitation":** Tech companies shield themselves behind the **"Fair Use" doctrine**, claiming that mining does not target the work itself but rather analyzes the underlying digital data. However, modern trends (especially in **2025 legislation**) have begun to distinguish between mining for scientific research (which is permitted) and mining for commercial purposes. The latter is considered an infringement on the author's **"potential market,"** as the machine becomes an economic competitor to those from whose works it learned[3].

- **The "Opt-out" Technical Strategy:** A new legal dilemma has emerged regarding whether a creator is obligated to tag their work with a **"No Mining"** label. Does silence constitute consent? Recent trends indicate that **protection is the default**, and mining without explicit **"Opt-in"** authorization is considered piracy disguised by algorithms[4].

Second: The Crisis of "Originality" in AI Outputs

The crisis emerges when Artificial Intelligence generates text or images that simulate the style of a specific artist without direct copying, causing traditional infringement standards—which rely on "substantial similarity"—to collapse.

- **The Concept of "Originality" Between Human and Machine:** Traditionally, "originality" is linked to the "personal imprint" of the human author. However, AI produce outputs characterized by apparent novelty but lacking "independent creative effort." The crisis lies here: if a machine produces a literary text mimicking the style of "Naguib Mahfouz" with stunning accuracy without copying a single sentence verbatim, should this be considered a new creation or a "moral reproduction" of the work's essence?[5]

- **The Theory of "Derivative Works" and Generative Algorithms:** AI outputs are often regarded as unauthorized **"Derivative Works,"** as they would not exist without the "digital digestion" of protected original works. The originality crisis is manifested in the fact that current laws protect the "expression" (form) rather than the "style," leaving the creative traits of human authors vulnerable to the machine's absolute capacity for simulation[6].

- **Lack of Legal Protection for Automated Outputs:** Recent judicial rulings have confirmed that outputs lacking **"substantial human direction"** fall into the **Public Domain**. This crisis has created a legal vacuum; neither the original creator is protected from simulation,

[2] Dr. Tariq Mahrous, *Artificial Intelligence and Copyright: A Study in Light of Modern Digital Legislation*, Dar Al-Nahda Al-Arabiya, Cairo, 2024, p. 115.
[3] See: U.S. Supreme Court, *Warhol Foundation v. Goldsmith* (Interpretation of Transformative Use), a ruling on which several cases against AI companies in 2025 were based
[4] Dr. Leila Ben Mira, *Legal Regulation of Data Scraping in the Digital Environment*, Journal of Jurisprudence and Law, Algeria, Vol. 8, 2025, p. 42
[5] Dr. Jalal Wafaa Muhammadin, *Intellectual Property: Contemporary Challenges and Future Horizons*, Mansha'at al-Ma'arif, Alexandria, 2023, p. 204.
[6] Gervais, D., *The Machine as Author: What AI Means for Intellectual Property*, Oxford University Press, 2024, p. 89.

nor does the AI user own the rights to what is produced. This encourages digital chaos that threatens the economic value of human creativity[7]

Third: The Difficulty of Digital Evidence (Proof)

In an environment reliant on **Deepfakes** and complex data chains, it becomes increasingly difficult to prove ownership of original content or trace the source of leaks. When AI simulates a style without direct reproduction, traditional infringement standards based on "substantial similarity" effectively collapse[8]

Section II: Modern Technical and Contractual Protection Strategies

As traditional law struggles to keep pace with real-time digital shifts, protection is evolving from "legal text" into "programmable code."

First: Blockchain and Decentralized Documentation (NFTs 2.0)

Non-Fungible Tokens (NFTs) are no longer merely for trade; they have become digital title deeds that document a work's history from its inception, facilitating the tracking of infringements[9]

- **Data Poisoning as a Deterrent Tool:** This strategy is one of the latest technical defense mechanisms. Creators use tools like **Nightshade** and **Glaze** to introduce microscopic changes into the digital file (text or image) that are imperceptible to humans but cause "semantic chaos" for AI models attempting to scrape them. If a model tries to train on this data without authorization, the "digital poison" degrades its generative capabilities, making piracy economically unviable[10]

- **Steganographic Watermarking (Invisible Fingerprinting):** This technology surpasses traditional watermarks that are easily removed. Ownership data is embedded within the deep "frequencies" or "codes" of the work. These fingerprints remain attached to the work even if it is cropped, modified, or reproduced by AI, facilitating **"digital forensic inference"** to prove the original source in court[11]

Second: Smart Contracts

Smart contracts allow creators to receive a percentage of profits automatically whenever their work is reused or traded, eliminating the need for intermediaries or complex litigation[12]

- **Decentralized Documentation and Trust Chains: Blockchain** technology provides a tamper-proof "digital criminal record." Once a work is registered on the blockchain, the creator

[7] U.S. Copyright Office (USCO) Decision regarding "Refusal to Register Works Generated Entirely by Artificial Intelligence," March 2025 Bulletin.
[8] See: French Court of Cassation (Cour de cassation) Decision on the Reproduction of Artistic Style, Case No. 23-112, issued January 2025 (Unpublished in Arabic).
[9] Eng. Sami Al-Harithi, *Blockchain Technologies and Their Applications in Copyright Protection*, Arab Technical Journal, Vol. 12, No. 3, 2025, p. 88.
[10] Dr. Samer Youssef, *Cybersecurity for Intellectual Property: Content Defense Techniques in the AI Era*, Arab Center for Research and Policy Studies, Doha, 2025, p. 210.
[11] Dr. Maryam Al-Shammari, *Technical Protection of Copyright in the Digital Environment: A Study of Means and Effects*, Journal of Law, Kuwait University, Vol. 49, No. 2, 2024, p. 85.
[12]Lucero, M., *Smart Contracts and IP Law: A New Era of Enforcement*, Journal of Cyber Law & Policy, Vol. 9, No. 2, 2024, p. 210.

receives a **Timestamp** certificate proving their creative priority, reducing the loss of rights in cross-border digital environments[13]

Automating Rights via Smart Contracts: Smart contracts represent a revolution in copyright management; they are self-executing codes that trigger automatically upon certain conditions. For example, a work can be programmed to remain inaccessible or unusable for AI training until a licensing fee is paid directly to the author's digital wallet. This transforms intellectual property from a "dormant right" awaiting a court rulin

Detailed Analysis: Smart Contracts as Governance Protocols

Smart contracts are not merely payment tools; they are **"Governance Protocols"** that grant creators full sovereignty over their works within the cross-border digital environment.

1. Granular Micro-Licensing

Smart contracts allow for the fragmentation of exploitation rights into extremely small units.

- **Detail:** An author can program a smart contract to permit specific types of usage—such as "Algorithmic Training only" or "Digital Display only"—at varying price points. This system eliminates the "all-or-nothing" approach of traditional licensing, creating a flexible marketplace where payments are made per **"Creative Consumption Unit."**

2. Provenance and Chain of Title

Blockchain provides an unbreakable **"Chain of Trust."**

- **Detail:** Every smart contract carries a comprehensive history of every modification, sale, or license. In the event of a legal dispute, the author does not need to prove ownership through witnesses or physical documents; instead, they present the **"Cryptographic Hash,"** which serves as a technical forensic record proving priority of innovation and the exact nanosecond of registration.

3. Autonomous Enforcement

The shift from a "right that requires a judge" to a "right that enforces itself."

- **Detail:** Digital works are designed to be **"Encapsulated"** via code. An AI model cannot "decrypt" the material or train on it unless the smart contract responds to the "License Request" (**Access Token**) after verifying the fee payment. Here, the software code acts as the **"Gatekeeper"** that prevents infringement before it occurs, rather than pursuing litigation after the fact.

4. Resale Royalties (Droit de Suite)

One of the most significant gains of smart contracts is the right of financial tracking.

- **Detail:** In traditional law, an artist loses their financial connection to their work after the first sale. Through smart contracts, the agreement is programmed to automatically return a

[13] Eng. Khaled Selim, *Blockchain and the Future of Legal Documentation*, Dar Al-Maaref, Cairo, 2024, p. 132

percentage (e.g., 10%) to the original author during every future resale in **"Secondary Markets."** This ensures long-term financial sustainability for human creators against the infinite digital flow.

- g into a "practiced right" protected by code [14]

Third: The Legislative-Technical Approach (Mandatory Labeling)

- **Algorithmic Transparency:** Modern legislation, such as the **EU AI Act 2025**, imposes technical obligations called **AI-DRM** (AI Digital Rights Management). These laws require companies to place a digital tag on all "machine-generated" content to distinguish it from human creation, protecting the market value of authentic human ingenuity[15]

- **Digital Collective Licensing Systems:** The future trend points toward AI-driven intermediary platforms for **Real-time Licensing**. These platforms link creator databases to training engines, calculating compensation based on the "creative contribution percentage" in the machine's output[16]

The core philosophy of this approach is to adapt software code to serve legal mandates, transforming intellectual property from a "static text" into an "embedded protocol."

1. Structural Level: "Protection by Design"

Drawing from the "Privacy by Design" principle in the GDPR, AI systems must incorporate "IP Protection by Design."

- **Universal Opt-out Protocols:** Legislation must mandate that AI developers program their **Web Crawlers** to automatically recognize and respect IP tags, such as the no-ai field in robots.txt files or image metadata.

- **Immutable Data Provenance:** Companies must be legally required to create a technical **"Black Box"**—a precise, unalterable log of all training data. This ledger serves as an official legal document required for the registration of any AI model with copyright and patent offices.

2. Procedural Level: Smart Mandatory Labeling

Labeling is no longer just a visual mark; it is a **"Digital Birth Certificate"** for content.

- **Bilateral Labeling:**

  - **Input Tagging:** Tracking human-authored works used in the training process.

  - **Output Tagging:** Embedding **"Cryptographic Watermarks"** in every text or image generated by AI.

[14] Lucero, M., *Code as Law: Smart Contracts in the Age of Generative AI*, International Review of Law, Computers & Technology, Vol. 38, Issue 1, 2024, p. 44.
[15] European Union, *Regulation (EU) 2024/1689 (AI Act)*, Official Journal of the EU, 2024.
[16] Dr. Omar Al-Obaidi, *Digital Intermediation in Copyright Management: Towards a Global Licensing System*, Dar Al-Nahda Al-Arabiya, Beirut, 2026, p. 55.

- **Legal Weight of Labeling:** New legislation should stipulate that **"the absence of a digital label on machine-generated output results in the immediate forfeiture of protection."** Such outputs would instantly fall into the **Public Domain**, technically forcing companies to comply with labeling to protect their commercial interests.

3. Contractual Level: Automated Collective Licensing

The crisis of millions of creators is solved through **"Legal Automation"** rather than endless litigation.

- **Sovereign APIs:** The state or IP authorities establish a centralized **API** containing fingerprints of protected works. The law mandates that AI companies interface with this API in real-time.

- **"Pay-per-Knowledge" System:** When a generative algorithm produces content mimicking a protected style, a **Smart Contract** automatically deducts **Micro-royalties** and distributes them to the rightsholders based on a "proportional contribution algorithm."

4. Punitive Level: Direct Technical Liability

- **"Legal Poisoning" Penalty:** If a company is found to have bypassed technical protections (e.g., circumventing tools like **Glaze** or **Nightshade**), it shall be classified as **"Aggravated Piracy,"** warranting the revocation of the model's license, not just a financial fine.

- **Shift in the Burden of Proof:** If a creator claims their style has been replicated but cannot prove it due to **"Algorithmic Opacity,"** the law requires the company to disclose **"Data Weights,"** demonstrating the extent of the model's reliance on that creator's work.

Model Legal Article

"The deployment of any Generative AI system in the digital market is prohibited unless it incorporates an 'Algorithmic Transparency Protocol' that enables training source tracking, ensures the labeling of outputs with indelible cryptographic watermarks, and maintains a mandatory link to automated collective licensing platforms to guarantee fair compensation for human creators."

Conclusion:

In conclusion, intellectual property protection is no longer merely a traditional legal matter; it has become a fundamental pillar of the rapidly accelerating digital economy. A successful future strategy depends not only on the rigor of laws but on their ability to adapt to emerging technologies such as Artificial Intelligence and **Blockchain**. Protecting digital creativity is the true investment to ensure the sustainability of innovation and safeguard the rights of future generations in a world that recognizes no geographical borders.

Strategic Recommendations

Accordingly, we propose the following set of recommendations:

1. **Updating Legislative Frameworks:** Drafting flexible laws that address emerging issues, such as ownership rights for AI-generated content and defining the legal liability of digital platforms.

2. **Adopting Modern Protection Technologies:** Relying on **Blockchain** technology for immutable ownership documentation and tracking digital works, alongside the use of **Digital Fingerprinting**.

3. **Enhancing International Cooperation:** Since the digital space is cross-border, international treaties must be activated, and technical and legal standards must be unified to combat transcontinental cyber-piracy.

4. **Promoting Digital Awareness:** Launching awareness campaigns targeting both users and creators to define their rights and duties, fostering a culture of respect for intellectual property as both a moral and economic value.

5. **Developing Dispute Resolution Mechanisms:** Establishing specialized digital platforms for rapid arbitration in intellectual property disputes to avoid lengthy judicial proceedings that do not keep pace with the speed of the digital age.