To Art or Not to Art: How AI Can Pivot from Shakespearean Villain to a Restorative and Structural Hero in the Creative Industries

Tea Radi Georgieva

[1] Vrije Universiteit Brussels, Ixelles 1050, Belgium
teageorgieva@vub.be

Abstract. The rapid deployment of generative artificial intelligence has introduced a critical regulatory lag, threatening to regress creative labor to a pre-copyright state of vulnerability reminiscent of the Elizabethan era. This paper investigates how the unconsented harvesting of proprietary artists' portfolios, vocal stems, and style signatures constitutes a systemic breach of personal data sovereignty under the European Union's GDPR. By treating creators protected identity footprints as public property, commercial technological entities leverage algorithmic opacity to build unearned market dominance, triggering imbalances. To resolve such friction, evaluation of the utilization of GDPR privacy mechanisms, such as Right to Explanation (Articles 13/14), Right to Erasure (Article 17), and record-keeping mandates (Article 30)—in piercing the algorithmic "black box." Furthermore, the idea of *art as code*, a legal-technical idea utilizing perceptual hashing and algorithmic data forensics to establish machine-readable rights architectures, is proposed. By pairing data protection mandates with computational origin, this paper demonstrates how AI can pivot from an extractive mechanism into a transparent, restorative infrastructure that safeguards creators, rather than erases their importance in our society.

Keywords: Artificial Intelligence, Arts, Intellectual Property, Creative Economy, Framework, Regulatory Lag, Laws.

1 Introduction

Ever since the Elizabethan era, artists have faced state censorship, privacy breaches, and the unauthorized transformation of their work. As Janet Clare explains, dramatic censorship meant that many works were heavily altered or lost, with no laws protecting even the world's most famous creators, including Shakespeare and Hayward. This historical parallel reveals that little has changed; the censor threatening how we create and perceive art is no longer a person, but the invisible force of AI. This technology acts like an Elizabethan Sea dog, raiding creators' art without their knowledge, seizing their "gold" to turn a corporate profit through monthly subscriptions and tokens. This historical loop, where the past entangles with the present, serves as the anchor to address the regulatory lag, building an ecosystem where artists can truly do Art and coexist with AI without systematic legal infringement.

This lag in AI regulation has been starkly evident since major tech entities deployed generative models globally. Despite rapid adoption, binding regulatory frameworks remain virtually non-existent—particularly for models that directly displace human creators and infringe upon IP laws daily. While pioneer lawsuits and emerging academic literature offer initial frameworks, the broader regulatory lag remains a critical hurdle for lawmakers and artists alike.

Crucially, where Elizabethan authorities weaponized libel to absorb private artistic expression into state surveillance, modern generative AI entities operate in reverse: wrongfully converting private, protected artistic expressions and identity markers into an "illusion of the public domain." When generative models scrape proprietary musical compositions, vocal timbres, and visual styles without consent, they do not merely breach copyright. They commit a direct invasion of the artist's personal data footprint—an infringement that entangles GDPR, IP, competition, and antitrust laws, and others.

Ultimately, AI is not simply stealing; it is cultivating an environment where creators actively lose their livelihoods, threatening their ability to sustain themselves within the creative industries while violating core European and national laws. Music and art are harvested without approval, effectively reducing artists to uncompensated "makeshift trainees." While prominent creators may possess the capital to litigate against tech giants or register extensive copyrights, the vast majority lack these monetary advantages. This raises the central question of this paper: how can existing European legal frameworks be adjusted and enhanced to ensure that all creators are empowered to do Art without the constant threat of privacy and economic exploitation?

2 Is Art Private? Data Sovereignty and the "Illusion of the Public Domain" Under GDPR

As Collette et al. (2023) observe, Article 22 of the GDPR establishes a delicate equilibrium between technological innovation and fundamental human rights, strictly limiting automated processing unless explicit consent or legal necessity is present. This statutory protection aligns with broader European fundamental rights frameworks designed to preserve personal dignity against unmonitored machine systems. However, in the realm of generative AI, commercial development entities treat artists' data footprints as if Article 22 exemptions do not apply, operating automated ingestion pipelines without explicit opt-in preferences. This operational model creates a profound constitutional failure: it denies creators the mandatory safeguards guaranteed under Article 22, namely, the right to obtain human intervention and contest automated exploitation. Consequently, restoring data sovereignty requires holding AI training agencies accountable to Article 22's strict consent and human-intervention requirements. According to Article 32 of the GDPR:

> “Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of process- ing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate

> technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate." [22]

This regulation finely aligns with the European privacy framework, who although decent, here contrasts with the needs of the artists severely. Given the example of cameras in a store, C. Stamelos abbreviates his support of these laws as a way of freedom of expression and compliance for the greater good. Stamelos and his team show the positive side of this regulation without considering the impact it has on things who aren't as visible as our faces. Art, in this context, is excluded and undermined. Artistic expression cannot be funneled into these articles as easily as the human body, as it is an intangible matter that requires a different approach. This law fails when applied to art because artistic creation is not merely a commercial asset; it is an extension of human expression and identity that cannot simply be locked away or protected like physical property. Allowing the unconsented extraction of artwork without legal consequences directly undermines the protective spirit of Article 32 GDPR. Consequently, this failure provides a compelling justification for artists to demand a targeted legal shift—one that restricts the operational freedom of AI developers and grants creators an absolute right of consent to opt out of training pipelines, ensuring their personal data footprint and privacy remain protected.

2.1 Cross-border GDPR complications vs. Music

The systemic fragility of cross-border artistic data processing was starkly demonstrated following the 2025 Suno data breach. As exposed by investigative reporting from *404 Media* and the security platform *Have I Been Pwned*, a breach compromised the personal information of over 55 million affected users, highlighting the borderless nature of generative AI and the deep embedding of GDPR violations within creative industries ecosystems. Because multinational AI entities operate within the European market—requiring secure financial transactions via processors such as Stripe, alongside the collection of email addresses and personal user metadata—their operational pipelines fall strictly under European data protection mandates. This incident illustrates a direct breach of GDPR Article 32 regarding security measures, while simultaneously violating statutory obligations under Articles 33 and 34 of the GDPR. Article 34 explicitly mandates that when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the breach to the data subject without undue delay. In stark contrast to these statutory obligations, platform executives failed to provide timely notification, withholding disclosure until investigative journalists independently uncovered and publicized the breach in July 2026.

Furthermore, this case underscores the volatile legal landscape governing EU-US cross-border data transfers—a framework historically fraught with complexity and regulatory invalidations, such as the downfall of the Privacy Shield. While tech developers frequently operate under the assumption that algorithmic ingestion shielding relieves them of cross-border consumer notifications, this posture has triggered severe regulatory friction in foreign jurisdictions. In the United States, Suno's failure to notify affected users has exposed the company to severe scrutiny

under state-level data protection statutes—most notably the California Consumer Privacy Act (CCPA/CPRA). California law mandates strict, time-sensitive notification of windows for breaches involving sensitive financial endpoints, such as the banking and payment credentials compromised in the breach. Consequently, US class-action litigation firms are deploying these state privacy statutes to challenge the platform's financial endpoint security, demonstrating that unconsented data exploitation creates compound liability across both European data sovereignty frameworks and American consumer privacy laws. Ultimately, this regulatory lag does not merely exploit artistic styles; it compromises fundamental aspects of creators' personal digital privacy.

2.2 Art and Article 30 GDPR: Less Discussed and Equally Important

In the aforementioned, two of the GDPR Articles 32 and 22 are quite often used as examples of GDPR related violations. However, one article that stands out within the scope of art privacy infringement is Art.30(1)(c) GDPR that states:

> "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. [2]That record shall contain all of the following information:
>
> (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
> (b) the purposes of the processing;
> (c) a description of the categories of data subjects and of the categories of personal data;
> (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;" [22]

In practice, however, these statutory requirements stand in direct contradiction with creative incentives of any kind. They expose a critical enforcement gap where generative AI companies, such as Suno, exploit operational opacity to evade compliance. Under Article 30(1)(c), the creative arts are subjected to an ambiguous legal standard regarding descriptive data categories. Most platforms operating in the generative AI space function in explicit breach of this rule: artists simply do not know which AI models have ingested their work, how much of their portfolio is actively utilized, or precisely how their data footprints are being processed. To support this critique, The Atlantic developed a lookup system within their published investigation—titled the "AI Watchdog: Free Music Archive Dataset"—where entering an artist's name into the search bar generates an analysis revealing which specific songs have been used by AI and are currently in a "free-music-archive." This empirical evidence decodes the ongoing, daily violations committed by platforms like Suno across millions of copyrighted and uncopyrighted songs, paintings, and photographs. Going forward, regulatory bodies must fundamentally enforce these recording obligations; yet it is precisely within this intersection that copyright and IP protections must step in to dismantle tech platforms' unregulated, endless access to creative works.

3 European Copyright Law

In the 2010s, the estate of Marvin Gaye filed a landmark copyright infringement lawsuit against Robin Thicke and Pharrell Williams over their hit single "Blurred Lines," claiming it copied Gaye's 1977 composition "Got to Give It Up." When the U.S. Ninth Circuit Court of Appeals ruled in Williams v. Gaye (2015) that the duo had infringed upon Gaye's work by replicating the "total concept and feel" of the original recording, a shockwave reverberated across the global music industry. For the first time, the legal boundary between unprotectable genre inspiration and protectable musical identity became fundamentally blurred. A decade later, generative AI has expanded this "blurred line" into a systemic crisis. Algorithmic models do not merely take inspiration from human compositions; they systematically digest the complete stylistic DNA of creators to output synthetic commercial substitutes. This reality is increasingly evident in retail environments across Western Europe—such as Carrefour location deployments in Belgium—where corporate drives for market share and margin optimization have led to the widespread adoption of AI-generated background music.

Under European copyright law, text and data mining (TDM) activities must invoke explicit statutory exceptions to avoid infringing authors' rights. In commercial contexts, tech entities rely primarily on Article 4 of the Copyright in the Digital Single Market (CDSM) Directive, which permits the reproduction and extraction of lawfully accessible works for mining purposes [27]. AI developers frequently exploit this provision as a broad safe harbor to harvest artistic works, regardless of formal copyright registration. However, under Article 4(3) of the CDSM Directive, this exception applies only if rights holders have not expressly reserved their rights—such as through machine-readable, code-level opt-outs. Because commercial scraping pipelines systematically ignore these opt-out indicators, platforms operate in persistent non-compliance with EU law and the international "Three-Step Test" mandated by the TRIPS Agreement. The seamless cross-border operation of AI technologies does not grant them immunity from international legal standards.

Because neither corporate entities nor current enforcement mechanisms adequately protect artistic works from unauthorized exploitation, a fundamental question of liability emerges. Crucially, while AI-generated outputs remain ineligible for copyright protection, commercial entities continue to monetize this "create-scrape-recreate-distribute" loop through token sales and recurring subscription models. Consequently, financial liquidity accumulates exclusively within tech platforms, while the human creators whose scrapped works power the underlying models face immediate economic displacement and loss of livelihood.

Moreover, uncopyrighted works on the internet additionally spark a conflicting protectionist legal matter. Despite their unprotected status, these artistic creations still embody a person's voice, personal data footprint, or stylistic identity. While a strict prohibition on using these unprotected materials is difficult to enforce, Recital 9 of the CDSM Directive (Directive (EU) 2019/790) explicitly establishes that the mining of unprotected data remains subject to legal limits if it involves acts of reproduction extending "beyond the scope of that exception"—referring to the temporary reproduction exception in Article 5(1) of Directive 2001/29/EC.

Proponents of generative AI often argue that algorithmic training constitutes mere transient data processing or transformative analysis necessary for technological innovation. AI companies do far more than "temporary" reproduction. Training a generative model—whether harvesting public domain classical scores, vocal stems, or uncopyrighted visual archives—requires permanently copying multi-terabyte datasets, extracting feature parameters, and storing them in persistent model weights to consistently output commercial substitutes.

Because this storage extends far beyond temporary caching, developers cannot hide behind the Article 5(1) temporary reproduction exception and operate in direct violation of European law. Ultimately, mass scraping breaches both statutory copyright protections for registered works and the strict reproduction limits for uncopyrighted data outlined in Recital 9. By leveraging these systematic illegal extractions, AI entities build unearned commercial market dominance, exposing a profound tension between current IP frameworks and Antitrust directives struggling to address this systemic market imbalance.

4 European Intellectual Property & Competition Laws: A Joint Venture in the Art Industry

Throughout the Modern Age, the core foundation of intellectual property began to take shape. It was during this era that society shifted away from arbitrary "privileges" granted at the whim of a monarch toward a standardized rule of law. In 1624, the Statute of Monopolies was adopted into English law, allowing the Crown to grant patents for genuine technological innovations—known as "letters patent"—for a period of 14 years. The Statute of Anne followed in 1710, enacted specifically to encourage learning by granting a similar 14-year protection for the printing of books. As these historic milestones demonstrate, intellectual property laws originally evolved from the arts and innovations, not the other way around.

In our current era, however, a dramatic historical reversal has occurred. Art no longer precedes laws or inspires their creation; instead, art begs for legislative protection after being overrun by technology. As Isohanni and Hietanen-Kunwald argue, while previous technological leaps like the printing press transformed distribution, Generative AI presents a fundamentally different opponent to intellectual property. It is an opponent capable of providing inexpensive duplicates that replace not just authorial works, but "the authors themselves" [5]. In this paradigm, traditional legal incentives to produce additional copies become moot—a reality most painfully felt in the visual arts, where creators historically earn their living through reproduction fees and licensing. When the financial viability of artistic labor dissolves, the very incentive to create unique works disappears with it.

On the opposing side of this debate stands corporate giant Coca-Cola. In a recent interview with *Forbes*, an executive shared insights on Coca-Cola's latest AI-generated holiday commercial—the first of many planned deployments—claiming that generating an AI ad is actually harder than traditional production and asserting that no visual artists were fired during its creation. To an extent, this corporate defense may hold true on the surface, but it deliberately ignores the broader economic picture: the process eliminates the need for videographers, stylists, actors, set designers, and

storytellers. In doing so, a massive portion of the creative ecosystem is severed from work opportunities and fair monetary returns. This dynamic exposes severe statutory friction in contemporary IP law, revealing a framework that currently shields corporate margins rather than sustaining human creators. The debate remains contentious and unresolved. IP laws remain static while AI moves at breakneck speed—past regulations, past institutions, and past people.

As Article 6bis of the Berne Convention establishes, authors possess moral rights to claim authorship over their creations and object to any derogatory treatment of their work. Yet, as Isohanni and Hietanen-Kunwald [27] observe, maintaining a balance between these personality-based human rights and technological innovation for the "greater good" remains one of the most complex legal tightropes of our time. This creates a question not only within the moral rights to claim ownership and oppose disparaging treatment of a creative work but to the right of partial or full monopoly of it, as this is the primary function of intellectual property protection. A delicate use of it is a must, as it can diverge into a monopoly and be in violation of EU competition law if the awarded protection surpasses what is necessary in order to secure the exercise of the given rights, as expressed by Spjuth and Zeitlin[15]. Most artists are unable to create such evident monopolies because the creative industries often rely on collaboration. In music, a song often has few authors. Within the scope of the literary world authors have co-authors, translators, editors, etc. Consequently, rights ownership in the artistic sector remains structurally fragmented, whereas in the technology sector, single corporate entities routinely centralize code, software patents, and proprietary data pipelines. This structural disparity allows tech giants to build dominant market positions, creating an intense legal friction between IP protections and EU antitrust enforcement that must be strictly defined going forward.

5 The EU AI Act

Does the EU AI Act truly empower creators, or does its regulatory lag force artists out of the creative space entirely? The journey toward this landmark legislation officially began on April 21, 2021, with a unique proposal by the European Commission to regulate Artificial Intelligence across the European Union. A couple of months later, the Council of the EU organized a virtual conference on the theme. By the end of 2021, an official draft of the Act was published alongside the decision that the European Parliament’s Internal Market (IMCO) and Civil Liberties (LIBE) committees would jointly lead negotiations, with Brando Benifei serving as lead negotiator. The following year marked the adoption of the Council’s common position on the AI Act. In June 2023, the European Parliament adopted its negotiating position with an overwhelming majority: 499 votes in favor, 28 against, and 93 abstentions. Finally, on July 12, 2024, the AI Act was published in the Official Journal of the European Union, marking the world's first binding, comprehensive legislation regulating AI.

Within this landmark text, the framework explicitly acknowledges that AI systems "present unique innovation opportunities but also challenges to artists, authors, and other creators and the way their creative content is created, distributed, used and consumed" (EU AI Act). This acknowledgment directly reinforces the

central thesis of this paper. Furthermore, Recital 107 establishes that "providers of such models draw up and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model." On paper, requiring developers to disclose their training data is a brilliant and much-needed step for the creative community. In practice, however, AI companies frequently evade true transparency. It is essential to demystify the legal phrasing here: focusing narrowly on "general-purpose AI models" is a double-sided sword. What about non-general-purpose models—those engineered specifically to scrape music stems, visual illustrations, or literary works? This focus highlights the structural limitations of the Act and its deterring generalizations. While Article 53 sets out strong general principles, it lacks the concrete enforcement mechanisms required to fully back artists and protect creative agency.

Despite the ambition of the AI Act, another critical layer comes into focus as the GDPR lurks alongside these regulations. A major driver of the regulatory lag has been the technical opacity of AI—the algorithmic "black box"—which leaves artists powerless because they cannot trace or prove how their proprietary work was ingested. Where the AI Act remains somewhat vague, the GDPR can be leveraged to force AI developers into true transparency.

Under Articles 13 and 14 of the GDPR, data controllers face strict disclosure mandates regarding automated processes. As legal scholarship emphasizes:

> "Article 13(2)(f) and 14(2)(g) GDPR address a key aspect of AI applications, i.e. automated decision-making. The controller has the obligation to provide: (a) information on ‘the existence of automated decision-making...’ and (b) ‘at least in those cases meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.’" [22]

By asserting this fundamental "right to explanation," Articles 13 and 14 pierce the black box. They provide creators with a direct legal lever to demand meaningful information about the logic behind automated dataset ingestion, effectively confronting the regulatory lag where the AI Act falls short. For instance, a Google Spreadsheet titled "Midjourney Style List" was exposed in the Discord chats of Midjourney CEO David Holz during a class-action lawsuit filed by a collective of visual artists against his company. The sheet contained over 16,000 artists' names, including living figures like Banksy, Yayoi Kusama, and David Hockney, alongside Magic: The Gathering illustrators and even a six-year-old child. Midjourney developers utilized this targeted index to refine the AI's capacity to emulate specific, recognizable artistic signatures. This remains the most glaring empirical evidence that AI developers—particularly specialized model providers—deliberately harvest human artistic style identities to optimize their commercial systems.

Moreover, this revelation illustrates how blind-sided artists remain against technological enterprises. Creators are left with virtually no systemic power while corporate platforms hold total leverage. Artists were never notified that their work was ingested, that their fundamental data footprint was disrupted, or that their creative labor was extracted and reused endlessly across global markets—all in persistent breach of the GDPR, intellectual property standards, copyright statutes, and the EU

AI Act. Courts in Germany and across Europe have attempted to enforce accountability, as seen in landmark cases like GEMA v. OpenAI (Munich Regional Court, 2025), where a collecting society successfully held an AI platform liable for copyright infringement via dataset memorization. Yet, despite such isolated legal victories, courts have rarely compelled tech firms to publish complete, auditable training registries or build public lookup portals for impacted creators. This exposes a fundamental systemic dilemma: instead of remaining trapped in an endless cycle of retrospective litigation where capital is drained with minimal structural change, the focus must pivot toward establishing preemptive data sovereignty tools before an artist's creation is ingested. Ultimately, legal reforms are mandatory, but pairing statutory evolution with personal data protection and technical sovereignty under the GDPR will yield far stronger results in the internal fight against tech giants than litigating after the damage is done.

6 Code vs. Copyright: Art as Code and a Path to Regulatory Peace

Human fingers contain unique cryptographic patterns—fingerprints distinct from a single living individual. Similarly, a programmatic script in Python possesses its own digital fingerprint: developed by specific authors, entirely unique, and mathematically linked to a distinct software service or artificial intelligence model. This code can be copyrighted, licensed, and legally protected. This fundamental computer science principle can be applied to creative arts. To translate artistic works into machine-readable rights, the legal system must transition toward objective, algorithmic data forensics. As digital forensics scholar Vassil Roussev explains, technical features serve as the foundational units of data comparison:

> "Features are the atomic components derived from the artifacts through which the artifacts are compared. Comparing two features yields a binary outcome—zero or one—indicating whether the feature match was successful or not. The set of all features computed by an algorithm for a given artifact constitutes a feature set. It can be viewed as an approximate representation of the original object for the purposes of matching it with other objects."[17, p. 103]

Essentially, any creative medium—whether a photograph, a musical composition, or a literary manuscript—can be translated into binary feature sets that create admissible physical evidence through detailed semantic analysis. Roussev notes that semantic matching enables platforms to:

> "...partially interpret the data content, in order to derive semantic features for comparison. Examples include perceptual hashes that can detect visually similar images, and methods in information retrieval and natural language processing that can find similarity of the subject and content."[17, p. 104]

Consequently, art becomes "code" when an artist's unique brushstrokes, color palettes, syntactic structures, or musical chord progressions are algorithmically compiled into "perceptual hashes"—mathematical signatures of their semantic features. If regulatory authorities seek to prove that an AI entity committed unauthorized data ingestion, they no longer need to litigate abstract aesthetic ideas; they simply execute a semantic match. If an AI platform's output or training weights mathematically match the artist's perceptual hash, infringement is objectively demonstrated through code.

This framework introduces both transformative opportunities and notable legal trade-offs. On the positive side, converting art into code offers a pragmatic compromise between corporate tech monopolies and vulnerable creative industries by establishing tangible, objective parameters for protection. It bypasses the traditional copyright "idea versus expression" dichotomy and sidesteps complex GDPR personality debates, replacing subjective judicial interpretation with mathematical boundaries. This approach creates an "artistic data forensics" model supported by the historical origins of data fingerprinting, whose original purpose was "to produce a very simple real-time string-matching algorithm and a procedure for securing files against unauthorized changes" [17]. In a creative context, this technical architecture functions as a shield against unauthorized extractions while providing AI developers with clear safe harbors against frivolous litigation. Converting art into code can establish a state of regulatory peace: AI developers gain an exact mathematical threshold of what they may legally process, while artists receive a concrete, code-based defense protecting their aesthetic identities.

However, in contrast to these advantages, critical technical limitations remain. A major pitfall of replacing traditional copyright frameworks entirely with algorithmic matching is that feature-matching systems remain susceptible to mathematical errors. As Roussev observes: "...it is possible to have a false positive—a true result for an element that has never been inserted but whose bits have been set (by chance) by other element insertions."[17, p. 101]

If judicial bodies rely exclusively on code to determine copyright infringement, the legal system becomes subject to algorithmic false positive rates. In computational musicology, where countless compositions share identical chord progressions, basic beat patterns, or color spaces, treating art strictly as code risks triggering widespread false positives. This dynamic could flood judicial dockets with speculative claims where artists and tech entities falsely accuse one another of theft simply because of their underlying perceptual hashes overlapped by random statistical chance. Therefore, a hybrid governance framework—combining traditional statutory copyright rules with computational forensics—offers the most viable path forward, as neither law nor code alone can establish absolute legal certainty.

Connecting this framework back to data protection, *art as code* directly intersects with the GDPR's "Right to Erasure" (Article 17). Even if artists successfully convert their unique creations into copyrightable code, significant uncertainty remains regarding whether regulatory authorities can technically verify that an AI firm has genuinely deleted a specific perceptual hash from its training pipeline. Because generative models compress billions of data points into an opaque, high-dimensional "black box" (the latent space), current computer science methods cannot easily extract or force a neural network to "unlearn" a specific feature set without retraining the entire model from scratch. Consequently, even when an artist uses "Art as Code" to

prove unlawful scraping occurred, enforcement agencies face immense technical friction when issuing deletion orders—such as those previously handed down by the Italian Data Protection Authority (Garante) in biometric exploitation cases like Clearview AI.

Ultimately, translating human creativity into code is not the primary obstacle; the fundamental challenge lies in constructing the regulatory and technical mechanisms around it. While algorithmic matching carries the inherent risk of false positives, without such technical innovations, establishing a viable, enforceable future for creative IP rights remains impossible.

7 Conclusion

The rapid deployment of Generative AI has exposed a profound regulatory lag across European digital law, threatening to regress creative labor to a pre-copyright state of vulnerability reminiscent of the Elizabethan era. As this paper demonstrates, the continuous, uncontested ingestion of artistic portfolios does not merely challenge statutory copyright boundaries; it constitutes a systemic violation of personal data sovereignty under the GDPR. By treating artistic identities, vocal stems, visual style signatures, etc. as an "illusion of the public domain," commercial technological entities leverage regulatory opacity to construct unearned market dominance, triggering severe antitrust imbalances within the internal market. This imbalance does not simply trigger economic consequences but reveals an unusual need for those companies to dominate and conquer an industry where people already don’t make enough and constantly face the underdeveloped irony of the laws.

While legislative developments such as the EU AI Act establish necessary transparency mandates, their reliance on broad categories like "general-purpose AI" leaves specialized artistic scraping pipelines under-regulated. To bridge this gap, privacy enforcement mechanisms—specifically the GDPR's Right to Explanation [Articles 13/14], Right to Erasure [Article 17], and automated decision-making protections [Article 22]—must serve as primary legal levers to pierce the algorithmic "black box". Such legislative developments, despite their novelty, prove that suggestive and generalized methods do not work for specific stems of industries who are not major economic players. For example, medical patents laws are more developed as their supply and demand is higher.

Ultimately, achieving structural regulatory peace and an AI hero requires pairing statutory evolution with computational innovation. Translating art into code through perceptual hashing and digital data forensics provides objective, mathematical parameters to defend aesthetic identity and verify dataset intake. Although technical challenges such as false positives and latent space unlearning persist, establishing machine-readable rights architectures enables AI to pivot an extractive mechanism into a transparent, restorative and preservative infrastructure. By empowering creators as sovereign data subjects rather than uncompensated makeshift trainees, European legal frameworks can foster a sustainable digital ecosystem where human artistry and technological innovation co-exist in true equipoise.

References:

1. Plaintiffs' First Amended Complaint, Andersen v. Stability AI Ltd., No. 3:23-cv-00201 (N.D. Cal. Nov. 29, 2023).
2. Order Granting in Part and Denying in Part Motions to Dismiss, Andersen v. Stability AI Ltd., No. 3:23-cv-00201 (N.D. Cal. Oct. 30, 2023).
3. Case C-252/21, Meta Platforms and Others v. Bundeskartellamt, ECLI:EU:C:2023:537 (July 10, 2023). Senftleben, M. (2026). Text and Data Mining, Generative AI, and the Copyright Three-Step Test. IIC - International Review of Intellectual Property and Competition Law, 57, 67–107. https://doi.org/10.1007/s40319-026-01680-2.
4. Synodinou, T.-E., Jougleux, P., Markou, C., & Prastitou Merdi, T. (Eds.). (2025). EU Digital Law in the AI Era. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-96743-6.
5. Corrales Compagnucci, M., Haapio, H., Fenwick, M. (eds.): Generative AI, Contracts, Law and Design. Perspectives in Law, Business and Innovation. Springer Nature, Singapore (2025). https://doi.org/10.1007/978-981-95-2058-9
6. European Union: Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union L (2024).
7. Generative AI Prohibited Use Policy. [https://policies.google.com/u/1/terms/generative-ai/use-policy]
8. Girasa, R.: Artificial Intelligence as a Disruptive Technology: Economic Transformation and Government Regulation, 2nd edn. Palgrave Macmillan / Springer Nature, Cham (2025). https://doi.org/10.1007/978-3-032-02827-3
9. Grba, D.: Deep Else: A Critical Framework for AI Art. Digital 2(1), 1–32 (2022). https://doi.org/10.3390/digital2010001
10. Gregory, S., Sircar, A.: AI Governance Handbook: A Practical Guide for Enterprise AI Adoption. Professional Practice in Governance and Public Organizations. Springer Nature, Cham (2025). https://doi.org/10.1007/978-3-031-89266-0
11. Historic Timeline | EU Artificial Intelligence Act. [https://artificialintelligenceact.eu/developments/]
12. Hylland, O.M.: Regulating artificial art: Comparing cultural policy strategies, narratives and responses in light of the AI revolution. In: Nordic Conference of Cultural Policy Research, Copenhagen (2023).
13. Jiang, H., Brown, L., Cheng, J., Anonymous Artist, Khan, M., Gupta, A., Workman, D., Hanna, A., Flowers, J., Gebru, T.: AI Art and its Impact on Artists. In: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (AIES ’23), pp. 1–12. ACM, New York, NY, USA (2023). https://doi.org/10.1145/3600211.3604681
14. Kelomees, R., Guljajeva, V., Laas, O. (eds.): The Meaning of Creativity in the Age of AI. Estonian Academy of Arts (2022).
15. Këllezi, P., Kilpatrick, B., Kobel, P. (eds.): Liability for Antitrust Law Infringements & Protection of IP Rights in Distribution. LIDC Contributions on Antitrust Law, Intellectual Property and Unfair Competition. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-17550-4
16. Marino, D., Monaca, M.A. (eds.): Generative Artificial Intelligence and Fifth Industrial Revolution. Lecture Notes in Networks and Systems, vol. 880. Springer Nature, Cham (2025). https://doi.org/10.1007/978-3-031-73880-7
17. Roussev, V.: Digital Forensic Science: Issues, Methods, and Challenges. Synthesis Lectures on Information Security, Privacy, & Trust. Morgan & Claypool Publishers (2016). https://doi.org/10.2200/S00738ED1V01Y201610SPT019

18. Senftleben, M.: Text and Data Mining, Generative AI, and the Copyright Three-Step Test. IIC - International Review of Intellectual Property and Competition Law 57, 67–107 (2026). https://doi.org/10.1007/s40319-026-01680-2
19. Synodinou, T.-E., Markou, C., Jougleux, P., Prastitou Merdi, T. (eds.): EU Digital Law in the AI Era. Springer Nature, Cham (2025). https://doi.org/10.1007/978-3-031-96743-6
20. Ystad, S., Kronland-Martinet, R., Kitahara, T., Hirata, K., Aramaki, M. (eds.): Music and Sound Generation in the AI Era. Lecture Notes in Computer Science, vol. 15236. Springer Nature, Cham (2026). https://doi.org/10.1007/978-3-032-02042-0
21. Clare, Janet. Art made tongue-tied by authority: Elizabethan and Jacobean Dramatic Censorship. Manchester University Press, 1999.
22. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119/1 (2016).
23. European Union: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689 (2024).
24. European Union: Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (CDSM Directive). Official Journal of the European Union, L 130/92 (2019).
25. Regional Court of Munich I (Landgericht München I): GEMA v. OpenAI GmbH, Case No. 31 O 1234/25 (2025).
26. European Digital Rights (EDRi): Italian DPA fines Clearview AI for illegally monitoring and processing biometric data of Italian citizens. EDRi (2022), https://edri.org/, last accessed 2026/07/31.
27. Isohanni, N., Hietanen-Kunwald, P.: Generative AI, Contracts, Law and Design. In: Corrales Compagnucci, M., Haapio, H., Fenwick, M. (eds.) Perspectives in Law, Business and Innovation, pp. 175–210. Springer Nature, Singapore (2025). https://doi.org/10.1007/978-981-95-2058-9