# AI system behavior on images involving personal data and IP rights

Oleksandr Muzychuk[1,†], Victoria Vysotska[1,†], Dmytro Pashniev[1,†], Daniil Shmatkov[1,2*,†], Olha Rozghon[2,†], and Denys Baranovskyi[3,†]

[1] *Kharkiv National University of Internal Affairs, L. Landau avenue, 27, Kharkiv, 61080, Ukraine*

[2] *Scientific and Research Institute of Providing Legal Framework for the Innovative Development, NALS of Ukraine, Chernyshevska St., 80, Kharkiv, 61002, Ukraine*

[3] *Rzeszow University of Technology, Kwiatkowskiego Street 4 37-450 Stalowa Wola, Poland*

**Abstract**

A computational approach has been developed to analyze the behavior of generative image models when processing user visual data containing intellectual property and personal data. The study aims to identify discrepancies between formally declared platform policies and the actual technical behavior of artificial intelligence models. The methods used include experimental modeling of image generation, semantic similarity analysis based on CLIP (ViT-B/32) embeddings, cosine similarity metrics, multivariate statistical analysis, and principal component analysis to assess the normative parameters of the platforms. The experiment covers four generative systems and includes a comparison of derived and transformative text instructions. The results demonstrate that the models inconsistently distinguish the legally significant distinction between derived and transformative uses and often generate higher visual similarities for "inspirational" queries. It is shown that the degree of similarity is determined predominantly by the internal architecture of the model rather than the semantics of the user query, which has significant implications for risk management in generative AI systems.

**Keywords**

generative image models; semantic embeddings; CLIP architecture; cosine similarity; multimodal machine learning; visual similarity analysis; algorithmic behavior; AI system evaluation.

## 1. Introduction and related works

Today, when the debates about who owns the rights to AI-generated works appear to be fading, another technical-legal question gains new relevance – how the rights of third parties are accounted for in such works. Such possible violations are reported by well-known writers, publishers, photographers, architects etc., and ordinary individuals. At the same time, users increasingly rely on generative tools without fully understanding how these systems interpret input images or what level of similarity they might reproduce. As visual models become more accessible, the gap grows between the user's expectations, the platform's formal restrictions, and the actual technical behavior of the model. This makes it important to examine how these systems operate.

Images and facial data require special legal attention because they enable immediate identifiability and trigger strict data-protection obligations [1]. Biometric data, including information relating to facial images, belong to those "sensitive" categories of personal data whose processing poses a heightened risk to an individual's rights and freedoms and therefore requires special protection. Resemblance to a real face becomes legally significant because it constitutes

*AIT&AIS-2025: Applied Information Technologies and Artificial Intelligence Systems, December 18-20, 2025, Chernivtsi, Ukraine*

* Corresponding author.

† These authors contributed equally.

o.muzychuk23@gmail.com (O. Muzychuk); victoria.a.vysotska@lpnu.ua (V. Vysotska); shmatkov.daniil@univd.edu.ua (D. Shmatkov); dvpashniev@univd.edu.ua (D. Pashniev); rozgon.olga.vl@gmail.com (O. Rozghon); denisbaranovskiy2@gmail.com (D. Baranovskyi)

0000-0001-8367-2504 (O. Muzychuk); 0000-0001-6417-3689 (V. Vysotska); 0000-0003-2952-4070 (D. Shmatkov); 0000-0001-8693-3802 (D. Pashniev); 0000-0001-6739-3927 (O. Rozghon); 0000-0002-6516-2794 (D. Baranovskyi)

biometric data, the processing of which requires consent and appropriate personal-data safeguards; otherwise, it may lead to a violation of the individual's right to privacy.

In addition, such works may contain various types of intellectual property. Therefore, we see that the issue is multifaceted and requires a comprehensive approach – both from the perspective of different areas of law and from the side of technology.

Today, the consumer relies on the platform, its algorithms, and its recommendations [2], the role of the human is diminishing [3], but AI does not eliminate liability, the outcome dominates over the user's intent [4]. And in this context, both biometric data and intellectual property emerge as areas of risk [4–8], and the level of transformation of the source image achieved through AI becomes a decisive factor here. Users also often think that the way they phrase the prompt will control the level of similarity and the legal risk. In actual use, the model does not always react to these differences. Even when the user clearly asks for a more distant or more creative result, the system may still generate an image that looks quite close to the original. Despite their theoretical "transformative" nature, generators sometimes reproduce elements or fragments of their training data [9] and similarity may arise even in the absence of any intent to copy [10]. In this direction, the views of scholars can be summarized as follows:

- Generative models produce similarity due to the statistical nature of training; high resemblance emerges as an architectural effect [4; 8–13].
- The user does not control the degree of similarity, because the model makes expressive decisions autonomously, although the user still plays a relevant role in the process [9–11].
- Models often do not recognize the distinction between derivative and transformative use, which creates legal uncertainty [7; 14].
- Similarity becomes a key legal factor in two domains simultaneously – intellectual property and personal data [5; 6; 10; 14–16].
- Images of a real person are automatically treated as highly sensitive data [5; 6; 17].
- Platforms formally declare differentiated risk categories, but the models themselves often fail to implement these distinctions [13; 15].
- The risks arise at both stages (input and output), but the visual output remains the primary source of legal exposure, even when the input appears legally safe [13; 18; 19].
- A significant part of the problem lies in the opacity of algorithmic decision-making: models do not reveal which features they consider relevant or how they weigh them, making the sources of similarity and identifiability impossible to verify or control [11; 16; 20].

Modern research highlights that visual content itself is becoming an important object of analysis in the digital environment [21]. The rapid development of image-generation systems shows that legal classifications are losing stability when confronted with technical behavior. Models trained on large-scale visual datasets reproduce structural patterns because of statistical proximity embedded in the architecture. As highlighted in the literature, generative systems rely on heterogeneous internal strategies, from shape, texture and layout analysis to semantic embeddings, most of which correspond to legal tests for distinctiveness, dominance, or likelihood of confusion.

Another systemic issue concerns the interaction between intellectual-property rules and personal-data regulation. The same generative behavior may produce legally neutral outcomes for abstract logos but high-risk outputs for human-centered trademarks, even under identical prompts. This becomes more evident when models generate close visual resemblance for tasks intended to create creative distance.

These developments show a more general problem: the law is built on clear categories and thresholds, but generative models follow their own internal logic and may not recognize these boundaries. This raises questions about how well platform policies match the actual behavior of the

models, whether they react differently to derivative and transformative prompts, and how this affects the overall risk.

The objective of this study is to determine whether image-generation platforms technically follow the legal distinction between derivative and transformative use, and to assess how this behavior interacts with intellectual property and personal-data risks. To achieve this, the research compares generative outputs produced under two legally meaningful prompt types, quantifies visual similarity to registered EU trademarks, and systematically evaluates platform policies across intellectual-property and personal-data criteria. The study aims to establish whether policy detail correlates with actual generative behavior and to identify how risk shifts when trademarks contain depictions of individuals. This type of input is particularly valuable for the study because it clearly involves personal data, copyright, and trademark rights.

## 2. Methodology

This study combined a review of platform policies with an experimental comparison of image-generation behavior. Both parts were carried out independently and later aligned through numerical analysis.

A dataset of nine trademarks was created using officially registered EU trademarks, balanced across three commercial positioning categories traditionally used in trademark research reflecting the depiction of men, women and children in the trademarks. All trademark files were downloaded from the official registry in a standardized format.

Each trademark was uploaded to four image-generation platforms: OpenAI, Artlist, OpenArt AI, and Pixlr. Two tasks were used for every trademark. The first instructed the model to "redraw this image and modify it slightly in a free artistic style", representing a higher-risk modification. The second asked the system to "create a different image inspired by this one", representing a lower-risk scenario. These task pairs were selected to reflect typical derivative-like and inspiration-based use cases.

The experiment should have produced seventy-two images (nine trademarks, four platforms, two tasks). One output failed, resulting in seventy-one valid images.

All collected files were processed in Python. Since image formats varied, the files were cleaned, standardized, renamed and aligned. To evaluate resemblance, among the various methods [22], we selected a semantic similarity measure based on the CLIP ViT-B/32 model. Each image was encoded into a normalised embedding, and similarity was calculated as the cosine similarity between two embedding vectors according to the following expression:

$$\mathrm{sim}(I_1, I_2) = \cos(E_1, E_2) \tag{1}$$

where $E_1$ and $E_2$ are the normalised CLIP embeddings of the two images, and sim is the cosine similarity score ranging from −1 to 1 (in practice, for image embeddings, values fell within the 0–1 interval).

Even small differences in sim reflect meaningful structural closeness because the embedding space captures semantic and compositional features rather than raw pixel values. This makes the metric suitable for assessing resemblance in both trademark and personal-data dimensions. For each platform, average similarity values were computed separately for the modification and inspiration tasks.

In parallel, the policies of the four platforms were systematically reviewed. A set of twenty-one criteria was constructed to capture how platforms address trademark issues, copyright issues and personal-data questions arising from user-uploaded images.

The following trademark-related criteria were coded:

- Whether the platform mentions third-party trademarks and prohibits uploading or generating copies or derivatives of protected marks.

- Whether the policy regulates the generation of logos or brand elements, and distinguishes between “inspiration/transformation” and “copying/similarity”.
- Whether fair-use exceptions, disclaimers or explanatory notes concerning trademark use are provided.
- The presence of a formal trademark complaint or takedown procedure.
- Whether the platform requires users to grant it a license over created trademark-related content.
- Allocation of liability for trademark or industrial-property infringements.
- Disclaimers stating that generated content may contain elements resembling protected marks.

Seven copyright-related criteria were coded:

- Whether the platform mentions third-party copyright and prohibits uploading or generating copies or derivatives of protected works.
- Whether the policy regulates generation involving copyrighted material and distinguishes inspiration from copying.
- Whether the platform provides fair-use, exception-related or similarity disclaimers for copyrighted works.
- The availability of a copyright-specific complaints or takedown mechanism.
- Whether users grant the platform a license to the generated work or content.
- Allocation of liability for copyright or other IP violations.
- Disclaimers stating that generated content may contain elements resembling protected works.

The following personal-data-related criteria were coded:

- Whether the platform prohibits or restricts uploading photographs of individuals.
- Whether facial images are treated as biometric data.
- Whether the platform prohibits identity recognition or facial identification.
- Whether user-provided facial images may be used for training.
- Allocation of responsibility for rights related to a person’s image.
- Whether biometric data can be deleted upon request.
- Whether “likeness” (visual similarity to a person) is treated as personal data.

This set covers the three main groups of risks (copyright, trademarks, and personal data) while remaining compact enough to allow consistent quantitative processing.

Each criterion was coded on a three-point scale (1 = clearly covered, 0.5 = partially covered, 0 = not covered). This produced a matrix of twenty-one variables for all four platforms. Variables with no variation across platforms were excluded before dimensionality reduction. The remaining variables were analyzed using principal component analysis to obtain continuous policy dimensions without assigning subjective weights.

The extracted policy components were subsequently aligned with the similarity measures obtained for each task, allowing both datasets to be evaluated within a unified analytical framework. Kendall’s coefficient of concordance was applied to test the internal consistency of the policy matrix and the similarity matrix, while pairwise correlations were used to examine potential associations between policy dimensions and generative behavior. All numerical transformations, preprocessing steps and statistical computations were carried out in Python.

## 3. Results

The results of the image comparison are presented in Table 1. In the table, we use the abbreviation "Re" for the prompt "Redraw this image and modify it slightly in a free artistic style", and the abbreviation "Ins" for the prompt "Create a different image inspired by this one."

**Table 1**
Similarity Scores for Redraw and Inspired Prompts Across Four AI Platforms.

| Trademark Nos | OpenAI | | Artlist | | OpenArt | | Pixlr | |
|---|---|---|---|---|---|---|---|---|
| | Re | Ins | Re | Ins | Re | Ins | Re | Ins |
| 003803591 | 0.74 | 0.77 | 0.86 | 0.75 | 0.81 | 0.87 | 0.48 | 0.49 |
| 009013558 | 0.69 | 0.73 | 0.77 | 0.80 | 0.83 | 0.90 | 0.34 | 0.33 |
| 017953534 | 0.66 | 0.90 | 0.87 | 0.73 | 0.78 | 0.87 | 0.43 | 0.54 |
| 001004927 | 0.65 | - | 0.83 | 0.74 | 0.84 | 0.84 | 0.40 | 0.42 |
| 018594683 | 0.73 | 0.74 | 0.83 | 0.78 | 0.83 | 0.61 | 0.39 | 0.38 |
| 014908628 | 0.77 | 0.80 | 0.81 | 0.83 | 0.79 | 0.75 | 0.42 | 0.42 |
| 013960216 | 0.77 | 0.78 | 0.65 | 0.67 | 0.77 | 0.78 | 0.47 | 0.50 |
| 015726491 | 0.83 | 0.87 | 0.94 | 0.78 | 0.86 | 0.84 | 0.46 | 0.51 |
| 005305032 | 0.75 | 0.86 | 0.89 | 0.80 | 0.85 | 0.76 | 0.49 | 0.52 |
| Average | 0.73 | 0.81 | 0.81 | 0.76 | 0.82 | 0.80 | 0.43 | 0.46 |

We identified the following variation between the two tasks ("Re" and "Ins"): OpenAI (0.08), Artlist (0.05), OpenArt (0.02), and Pixlr (0.03).

The average similarity of images to the trademarks was 0.71 for those depicting women, 0.68 for men, and 0.73 for children. It may be linked to biological, genetic, physiological, social, or behavioral factors, but it clearly requires a larger sample to draw any conclusions.

Table 2 presents the average values for the parameters examined in the policies and rules of the AI systems under review.

**Table 2**
Summary of Policy Detail Levels Across AI Systems

| Criteria | OpenAI | Artlist | OpenArt | Pixlr |
|---|---|---|---|---|
| Trademark Parameters | 0.64 | 0.43 | 0.50 | 0.43 |
| Copyright Parameters | 0.64 | 0.64 | 0.64 | 0.64 |

| | | | | |
|---|---|---|---|---|
| Personal Data Parameters | 0.79 | 0.71 | 0.71 | 0.29 |
| Average | 0.69 | 0.60 | 0.62 | 0.45 |

The principal component analysis (PCA), which reduces complex multi-criteria data into a smaller set of underlying factors, showed that over 82% of the variance in policy parameters is explained by a single dominant component representing the overall completeness and strictness of the rules. The remaining components contribute only marginally, capturing secondary differences in how specific categories of risks are regulated. Correlation analysis further demonstrated a strong positive association ($r > 0.90$) between the level of policy detail and the similarity scores, indicating that more comprehensive policies are linked to outputs that remain closer to the original trademarks.

## 4. Discussion

Research on visual data governance demonstrates that technical systems often fail to fully reflect legal distinctions, creating a gap between regulatory expectations and actual system behavior [1]. Our findings align with this observation, as the models reproduced identifiable visual features even when prompts were explicitly designed to reduce similarity. The main finding of this study is the identified pattern: the more detailed a platform's policies and rules are, the more accurately it generates derivative and transformative works. We see several possible interpretations of this phenomenon:

- The correlation between detailed policies and higher accuracy may be purely incidental. Legal and technical domains often develop in parallel rather than in coordination: lawyers expand policies without understanding model architecture, while engineers optimize outputs without fully considering legal thresholds [23]. This match can therefore look meaningful even if it emerges accidentally, without any causal link.
- Improved technical accuracy naturally pushes outputs closer to intellectual property and personal-data boundaries, and no policy can fully offset this. As models become more precise, they reproduce structures, proportions, or stylistic features that increasingly resemble protectable material. It is known that algorithms rely on different approaches (from shape, texture, and layout to semantic concepts) and the way they weight these features does not align with the legal assessment of distinctive and dominant elements in two images [8]. Legal rules simply cannot keep up with the speed of generative AI. As models become better and produce higher-quality outputs, they inevitably get closer to legally protected material, and therefore closer to potential infringement.
- Platforms recognize such risks and respond by increasing the granularity of their rules. The more accurate the system becomes, the more pressure it creates at the intersection of privacy and intellectual property, prompting platforms to expand their policies as a form of anticipatory risk management. The detail is less about guiding the model and more about protecting the platform by formalizing boundaries, disclaimers, and procedural safeguards.
- Regardless of how clearly platforms understand the underlying risks, they position themselves within a DMCA safe-harbor logic as they frame their role as service providers. This perception allows them to treat detailed policies as sufficient compliance, even when technical behavior of the model creates risks that the legal framework cannot fully mitigate. This aspect legally relates to copyright, although technically we see its extension to other areas. In addition, contemporary research already calls for the creation of an "AI harbor" that increases the responsibilities of data suppliers, model developers, and deployers [24].

Platforms with more detailed policies tend to deploy more mature and technically advanced models, which may explain why their outputs remain closer to the original images. Stronger policies correlate with systems that generate both more stable and more similar outputs, making these platforms simultaneously more compliant on paper and more exposed in terms of actual generative behavior. Interestingly, the system refused to generate an image based on a trademark depicting a  person in only one case.

An important technical observation is that platforms do not legally distinguish between "derivative" (create a similar work) prompts (high legal-risk) and "transformative" (be inspired by this one, but generate a different work) prompts (low legal-risk): on average, half of the examined AI systems produced more similar images for transformative prompts. Figures 1–3 illustrate one example of such generation.

As an example, a previously registered but no longer valid European trademark 009013558 [25] was used. The image was used exclusively for research purposes and was not employed for any commercial use.

Even when users intend to create more distance from the source, generative systems may still retain core visual patterns from the original image, so a certain level of similarity can appear simply as a result of how the model operates [16]. The terms "derivative" and "transformative" describe two different degrees of similarity between the original material and the generated output. A derivative work stays close to the source and repeats recognizable elements, while a transformative work introduces meaningful changes and creates a new expression based on the original idea. Although these terms originate from copyright law and are not formally applied in every jurisdiction, they work well as analytical categories across all three areas (copyright, trademarks, and personal data) when assessing the likelihood of infringement. But it is important to emphasize that legal liability arises from the (derivative-/transformative-) use of a work, not from the work itself, we are examining the conditions that lead to this.

**Figure 1:** Registered trademark No. 009013558 [25].

**Figure 2:** Derivative work generated using OpenArt AI (Similarity score: 0.77).

**Figure 3:** Transformative work generated using OpenArt AI (Similarity score: 0.80).

The distinction between data extraction and expressive duplication is a key criterion in this context, although the boundaries between them remain unstable [7]. In each field, a more derivative output signals higher legal risk, while a more transformative output significantly reduces it, but as shown in our findings, it does not remove the risk.

Our observation concerns the variability between the two tasks ("Re" and "Ins"). The platforms differed in how consistently they reacted to the change in prompt type. OpenAI showed the highest variation between tasks (0.08), followed by Artlist (0.05), while OpenArt (0.02) and Pixlr (0.03) remained comparatively stable. This variation can be treated as a technical indicator of model maturity: systems with more stable behavior across different prompt types tend to reflect more predictable internal representations, whereas larger swings suggest that the model does not consistently differentiate between derivative and transformative instructions. At the same time, the legal meaning behind our prompts was not taken into account by the model in its interpretation.

Another explanation for this inconsistency lies in the architectural priorities of modern generative models. Their optimization goals focus on making the image look coherent and consistent inside the model. Because of this, prompts that are very different from a legal point of view are treated almost the same by the system. The model follows the patterns it learned during training, so both tasks often produce images that follow similar internal routes in generation. This means that unless the system is specifically designed to avoid copying, it will often stay close to the original image. The model tends to keep the main shapes and visual structure, even when the user asks it to move further away. As a result, a derivative-like similarity can appear even when the prompt is clearly written to reduce legal risk.

This means that users cannot meaningfully reduce legal risk simply by rephrasing the initial prompt, since the model does not consistently align its behavior with the legal intent expressed in the wording.

This mismatch is also relevant for regulators. Relying on textual distinctions between derivative and transformative use may give the false impression that these categories can be enforced at the model level, while our results show that current systems do not follow these boundaries technically.

We acknowledge that the sample of prompts and platforms was small, which is a limitation of the study, but it also serves as an important signal both for the platforms themselves and for future research should such changes occur.

This result shows that the legal meaning of a prompt and the technical behavior of a model are not aligned. Even when a prompt explicitly signals low-risk creative distance, models frequently replicate structural features, proportions, or stylistic markers with equal or greater closeness than in explicitly derivative tasks. This means that the user's intention to reduce legal exposure does not reliably translate into safer outputs, because the model optimizes for visual coherence and latent-space proximity. The gap between legal wording and technical response creates a weakness –

platforms imply these verbal distinctions in their policies, but the models themselves do not actually follow or apply them when generating images.

In the context of these findings, it is important to clarify where the actual infringement risks arise. With respect to intellectual property (copyright and trademarks), most legal systems require some form of commercial use, alongside other factors, to establish a violation. This requirement is especially relevant for trademarks, which are registered for specific goods and/or services and are legally tied to commercial use in those categories. Personal-data rules work differently: commercial use may increase liability, but even non-commercial use almost always triggers legal obligations and potential sanctions [26-29]. Thus, for trademarks that depict individuals, the risk of infringement when using AI increases as the issue moves to personal data.

Moreover, as shown in previous studies, such trademarks are registered infrequently [30] and not always successfully, while copyright arises automatically once the originality threshold is met, and personal data require no threshold at all, they exist together with the person. The average standard lifespan of a trademark is ten years, with the possibility of renewal for the same period upon payment of the required fee. For example, the trademark shown in Figure 1 has already expired, while most of the other marks used in this study remain active. Copyright, by contrast, does not require renewal and continues throughout the author's lifetime and for seventy years after death, and personal data are protected for the entire lifetime of an individual without any additional formal steps. In light of these differences, the overall risk of trademark infringement in the light of our study appears comparatively lower.

This risk means that what begins as a trademark issue can quickly evolve into a personal-data problem when a model reproduces identifiable features of a real person. Trademark law tolerates a degree of similarity unless it affects commercial origin or consumer perception, but personal-data law treats identifiability itself as the trigger. Therefore, when AI systems generate outputs that resemble individuals, the primary exposure shifts from trademark infringement to personal-data misuse, expanding both the scope and the severity of potential violations.

A key limitation of this study is the opacity of the platforms' internal algorithms: we cannot observe the models' internal flags, decision pathways, or safety triggers, and therefore cannot determine which specific mechanisms influence similarity, identifiability, or the decision to reject an input. These systems operate as closed environments where only the final output is visible, while the underlying reasoning remains inaccessible. It shows that across all platforms and prompt types the experiment resulted in only a single refusal, even though the inputs simultaneously implicated personal data, copyright, and trademark rights. Because the technical logic behind these outcomes cannot be examined or verified, the study cannot offer concrete solutions; it can only signal the risks inherent in processing such composite inputs within opaque generative systems.

## 5. Conclusions

Although this study could be interpreted as supporting the claim that the user does not control the degree of similarity, we would prefer to reformulate this point from the previous studies as follows: the user carries additional responsibilities in reducing the level of resemblance, because we acknowledge that, with sufficient effort, this can in fact be achieved. Whether the user chooses to reach such a level or not remains a matter of individual decision. Likewise, blindly assuming that the model has produced a transformative work and that no infringement can arise is also ultimately a choice made by the user.

The results of this study suggest that current generative models do not consistently reflect the legal distinction between derivative and transformative use. Across platforms and prompt types, the systems tended to produce similar levels of resemblance, and in some cases even higher similarity for "inspiration" tasks. This indicates that the degree of transformation appears to depend more on the model's internal functioning than on the wording of the prompt. At the same time, even moderate visual similarity can retain legal relevance in both intellectual-property and personal-data contexts.

When a trademark contains the image of a real person, the input acquires a multi-layered legal character, combining trademark rights, copyright relevance and personal-data implications. In such cases, higher visual resemblance may increase the likelihood of legal concerns, particularly with respect to identifiability. While platforms describe risk distinctions in their policies, the models themselves do not always reflect these distinctions in their generative behavior. These observations indicate that the use of human-centered trademarks in generative systems calls for particular care, as the legal implications arise primarily from how the final image is rendered.

This study is constrained by the limited transparency of generative systems: their decision processes, internal thresholds and feature-weighting strategies remain inaccessible, and only the final output can be observed. As a result, it is not possible to determine why certain visual elements are retained, modified or ignored, nor how the systems interpret identifiability. In addition, the scope of the experiment was necessarily limited to a selected set of prompts, platforms and trademarks, which means that the findings reflect the behavior of the systems within this specific configuration rather than across all possible scenarios. These constraints require that the conclusions stay grounded in observable results and not rely on assumptions about hidden technical processes.

Future work may explore a wider range of platforms, model versions and similarity metrics, including embedding-based measures that capture semantic distance. Expanding the collection of trademarks depicting real individuals and comparing outputs across legal jurisdictions could provide a clearer picture of how generative systems interact with complex rights objects. Further work could also examine whether tools that increase transparency or check the image after generation can actually help reduce similarity and lower the related legal risks.

## Declaration on Generative AI

Generative AI tools (OpenAI, Artlist, OpenArt AI, and Pixlr) were used to generate images and ChatGPT 5.1 was used to assist in language editing, paraphrasing, and stylistic refinement of the manuscript. All conceptual contributions, data selection, methodological decisions, study design, interpretations, and conclusions were developed entirely by the authors. The authors reviewed and validated all AI-generated suggestions and takes full responsibility for the content of the final text.

## References


[1] M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst, Y. Qiao, Visual surveillance within the EU General Data Protection Regulation: A technology perspective, IEEE Access 7 (2019) 111709–111726. doi:10.1109/ACCESS.2019.2934226.

[2] D. Lim, Computational trademark infringement and adjudication, in: Research Handbook on Intellectual Property and Artificial Intelligence, Edward Elgar Publishing, 2022, pp. 259–289.

[3] R. Batty, Trade mark infringement and artificial intelligence, 2021. URL: https://ssrn.com/abstract=3978248.

[4] N. Cai, Research on the trademark protection of artificial intelligence generation technology achievements, Advances in Economics and Management Research 12 (1) (2024) 502–502.

[5] C. Kuraku, S. K. Rajaram, H. K. Gollangi, V. N. Boddapati, G. K. Patra, Advanced encryption techniques in biometric payment systems: A big data and AI perspective, Library of Progress–Library Science, Information Technology & Computer 44 (3) (2024) 2447.

[6] E. P. Galla, C. R. Madhavaram, V. N. Boddapati, Big data and AI innovations in biometric authentication for secure digital transactions, 2021. URL: https://ssrn.com/abstract=4980653.

[7] Y. Leibler, From infringement to innovation: Reimagining copyright for AI training datasets, 2024. URL: https://ssrn.com/abstract=4986763.

[8] R. Abbott (Ed.), Research handbook on intellectual property and artificial intelligence, Edward Elgar Publishing, 2022.

[9] A. Verma, The copyright problem with emerging generative AI, Journal of Intellectual Property Studies 7 (2023) 69.
[10] M. D. Murray, Generative AI art: Copyright infringement and fair use, SMU Science and Technology Law Review 26 (2023) 259.
[11] M. P. Goodyear, Who is responsible for AI copyright infringement?, Issues in Science and Technology 41 (1) (2024) 31–33.
[12] Z. Wang, C. Chen, V. Sehwag, M. Pan, L. Lyu, Evaluating and mitigating IP infringement in visual generative AI, 2024. arXiv:2406.04662.
[13] G. Liang, L. Lu, Enhancing data protection in AI-driven investment and robo-advisory services: A comparative analysis of EU and China regulatory approaches, Law, Ethics & Technology 2 (1) (2025) 1–22.
[14] M. Grynberg, AI and the "Death of Trademark", Trademark Reporter 114 (2024) 695.
[15] A. Kolasa, M. Panek, Z. Gajewska, Individuals facing biometric identification – an analysis of Article 5 of the Artificial Intelligence Act with particular reference to consumer protection, Internetowy Kwartalnik Antymonopolowy i Regulacyjny (Internet Quarterly on Antitrust and Regulation) 14 (1) (2025) 96–117.
[16] C. O. Mihăilă, M. Mihăilă, Video surveillance and Artificial Intelligence: How does it affect privacy and intellectual property rights?, Zbornik radova Pravnog fakulteta u Nišu 100 (2023) 189–222. doi:10.5937/zrpfn0-48197.
[17] C. Meurisch, M. Mühlhäuser, Data protection in AI services: A survey, ACM Computing Surveys 54 (2) (2021) 1–38.
[18] G. Sebastian, Privacy and data protection in ChatGPT and other AI chatbots: Strategies for securing user information, International Journal of Security and Privacy in Pervasive Computing 15 (1) (2023) 1–14.
[19] K. I. Lee, Study on the use and protection of biometric data under EU AI Act, Law Journal 85 (2024) 57–82.
[20] D. Almeida, K. Shmarko, E. Lomas, The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks, AI and Ethics 2 (3) (2022) 377–387.
[21] D. Shmatkov, M. L. Zagalaz-Sánchez, J. Cachón-Zagalaz, Analysis of posters for informing the population via social media during COVID-19: Ukrainian network, Psycholinguistics 30 (1) (2021) 249–273. doi:10.31470/2309-1797-2021-30-1-249-273.
[22] D. Shmatkov, O. Gorokhovatskyi, N. Vnukova, Elaborative trademark similarity evaluation using goods and services automated comparison, in: Proceedings of the 7th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2023), Kharkiv, Ukraine, April 20–21, 2023.
[23] Y. Lin, T. Guan, From safe harbours to AI harbours: Reimagining DMCA immunity for the generative AI era, Journal of Intellectual Property Law & Practice 20 (9) (2025) 605–616.
[24] C. M. Gray, R. Gairola, N. Boucaud, M. Hashmi, S. S. Chivukula, A. R. Menon, J. N. Duane, Legal trouble? UX practitioners' engagement with law and regulation, in: Companion Publication of the 2024 ACM Designing Interactive Systems Conference, 2024, pp. 106–110. doi:10.1145/3656156.3663698.
[25] European Union Intellectual Property Office (EUIPO), European Union trademark EM500000009013558, EUIPO eSearch database. URL: https://euipo.europa.eu/eSearch/#details/trademarks/009013558.
[26] O. Muzychuk, M. Nazarkevych, D. Shmatkov, Y. Onishchenko, D. Pashniev, and V. Svitlychnyi, "Unpacking the value of 'All Rights Reserved' on websites," CEUR Workshop Proceedings, vol. 4126, pp. 436–451, 2025. URL: https://ceur-ws.org/Vol-4126/paper21.pdf
[27] V. Vysotska, K. Smelyakov, A. Chupryna, D. Darahan, O. Torubara, and O. Shyshymenko, "Social engineering in Ukraine: Threats and intelligent detection approaches," CEUR Workshop Proceedings, vol. 4110, pp. 317–331, 2025. URL: https://ceur-ws.org/Vol-4110/paper24.pdf

[28] S. Chyrun and V. Vysotska, “Innovative virtual reality system for training in providing first aid in crisis and combat conditions of war using VR/AR technologies,” CEUR Workshop Proceedings, vol. 4126, pp. 377–435, 2025. URL: https://ceur-ws.org/Vol-4126/paper21.pdf
[29] V. Vysotska, D. Uhryn, O. Iliuk, Y. Ushenko, and V. Yatsyshyn, “Application of machine learning for predicting fraudulent anomalies in financial transactions,” CEUR Workshop Proceedings, vol. 4126, pp. 171–185, 2025. URL: https://ceur-ws.org/Vol-4126/paper12.pdf
[30] B. A. Keserű, “Trademark protection for faces? A comprehensive analysis on the benefits and drawbacks of trademarks and the right to facial image,” Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 15, p. 88, 2024.