Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 145

AI-Powered Trademark Enforcement and Online Intermediary Liability: Implications for the US and EU Regulatory Frameworks

Giuseppe Colangelo

2026

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Giuseppe Colangelo is a Jean Monnet Professor of European Innovation Policy and an Associate Professor of Law and Economics at University of Basilicata (Italy). He is a Senior Scholar at the International Center for Law & Economics (ICLE), and the Scientific Coordinator of the Research Network for Digital Ecosystem, Economic Policy and Innovation (Deep-In).
His primary research interests are related to competition law and policy, market regulation, innovation policy, intellectual property, and economic analysis of law.
Giuseppe has been a TTLF Affiliate since August 2017.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Giuseppe Colangelo, AI-Powered Trademark Enforcement and Online Intermediary Liability: Implications for the US and EU Regulatory Frameworks, Stanford-Vienna TTLF Working Paper No. 145, http://ttlf.stanford.edu.

Copyright

Abstract

The rise of artificial intelligence (AI) is expected to have an impact on intellectual property (IP) that may prove even more profound than that of the advent of the internet. Both developments, however, share a common feature: the increasing pressure placed on online intermediaries to adopt a more proactive role in the protection of IP rights. As with other disruptive technologies, AI generates both opportunities and risks, and may thus constitute simultaneously part of the problem and part of the solution. In the trademark context, while the expanding use of AI may open new avenues for infringing practices, the very same technologies also offer powerful tools to prevent, detect, and monitor the dissemination of counterfeit goods.

Table of contents

1. Introduction

Intellectual property (IP) is inherently sensitive to market and technological transformations, which generate new opportunities while simultaneously introducing novel risks. Globalization and digitalization, in particular, have enhanced efficiency and expanded consumer choice, profoundly reshaping supply chains and purchasing habits through increased industrial specialization and the exponential growth of online commerce. At the same time, these developments have exposed new vulnerabilities that facilitate IP infringement, creating fertile conditions for fraudulent actors to introduce counterfeit and unsafe goods into the market.[1] The substantial market value of IP-protected goods attracts organized criminal networks, resulting in a rise in counterfeiting and piracy, which not only cause significant revenue losses for IP rightsholders but also pose serious risks to consumer safety, public health, and environmental protection.

The emergence of generative artificial intelligence (GenAI), together with the integration of AI technologies into search engines, social networks, and e-commerce platforms, has already begun to transform the marketplace and is expected to exert an even more profound impact on IP protection.[2] While scholarly and policy debates have thus far focused primarily on the challenges posed by GenAI to copyright law, trademark law is

[1] See, e.g., OECD and EUIPO, 'Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges' (2025) https://doi.org/10.1787/94d3b29f-en (all the links have been last accessed on 15 January 2026).

[2] See, e.g., Robin Feldman, *AI versus creativity* (Cambridge: Cambridge University Press, 2025), reflecting on how the rapid expansion of AI puts pressure on the domains traditionally covered by the IP umbrella—namely invention (patent), expression (copyright), business information (trade secrets), and reputation (trademarks).

also likely to be significantly affected as GenAI becomes increasingly embedded in creative, marketing, and design workflows. AI lowers the cost and complexity of trademark fraud, as its capacity to rapidly and inexpensively generate imitative works or products that fall within the scope of trademark protection may erode the economic and signaling value of protected assets in this regime.

In parallel, the growing adoption and market penetration of AI assistants and autonomous agents are reshaping the role of human decision-making in consumer transactions.[3] These systems may not only influence purchasing choices by directing user attention toward specific brands, but may also independently navigate digital marketplaces, evaluate alternatives, and execute purchases.

[3] See, e.g., Amit Zac and Michal Gal, 'The Price of Advice: Experimental Evidence on the Effects of AI Recommenders', (2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5637090, providing empirical evidence of the ability of customized, consumer-facing AI recommender systems to influence purchasing behavior. For example, survey evidence indicates that, as early as 2024, a substantial proportion of European consumers had already engaged with generative AI chatbots for customer service, with adoption rates ranging from 82% in Spain to 69% in France: see ServiceNow, 'Share of consumers choosing to engage with Gen AI chatbots for customer service in Europe in 2024, by country', (2025) https://www.statista.com/statistics/1488691/engagement-with-gen-ai-chatbots-by-country-europe/.
Another survey conducted in 2024 across selected countries revealed that, while nearly six in ten Italian shoppers show the strongest preference for interacting with a customer service agent rather than seeking assistance from AI tools online, this proportion declines to 49% in the United States and 28% in Germany: see Core Media, 'Share of consumers who value human interaction with a customer advisor in selected countries in 2024', (2024) https://www.statista.com/statistics/1538414/consumers-preferences-for-human-interaction/.

As AI-powered assistants emerge as a central frontier of competition in online markets—and are widely expected to displace traditional search engines—the e-commerce sector is likely to undergo a gradual transition from keyword-based queries to conversational interactions. In this scenario, companies including Etsy, Shopify, and Walmart have entered into partnerships with OpenAI that allow users to browse and purchase products directly through ChatGPT.[4] The evolution of ChatGPT into a multifunctional shopping interface is further reinforced by its partnership with PayPal, under which users can complete transactions instantaneously via PayPal's digital wallet, while PayPal provides payment processing services for merchants using OpenAI's Instant Checkout functionality.[5] In response, Google has similarly partnered with firms such as Shopify, Etsy, Wayfair, Target, and Walmart to develop an open standard for agentic commerce.[6] This initiative supports integrated checkout functionality on eligible product listings within Google Search and the Gemini application, enabling users to complete purchases directly through AI-driven interfaces without the need to switch between applications or web pages.

---

[4] Bloomberg, 'Walmart Partners With OpenAI to Offer Shopping on ChatGPT', (2025) https://www.bloomberg.com/news/articles/2025-10-14/walmart-partners-with-openai-to-offer-shopping-on-chatgpt?taid=68ee4f30e3e28c000190c760&utm_campaign=trueanthem&utm_content=business&utm_medium=social&utm_source=twitter.

[5] PayPal, 'OpenAI and PayPal Team Up to Power Instant Checkout and Agentic Commerce in ChatGPT', (2025) https://newsroom.paypal-corp.com/2025-10-28-OpenAI-and-PayPal-Team-Up-to-Power-Instant-Checkout-and-Agentic-Commerce-in-ChatGPT.

[6] Google, 'New tech and tools for retailers to succeed in an agentic shopping era', (2026) https://blog.google/products/ads-commerce/agentic-commerce-ai-tools-protocol-retailers-platforms/.

As in previous waves of technological disruption, these developments test the boundaries and effectiveness of traditional property rights, offering new opportunities for expansion while simultaneously generating novel threats. In the context of trademark law, although AI technologies can substantially enhance productivity and foster growth by enabling the rapid creation of logos, slogans, brand names, and marketing campaigns, they also heighten the risk of infringement. In particular, AI-generated content that references or draws inspiration from existing trademarks may increase the likelihood of consumer confusion or contribute to the dilution of well-known marks. In parallel, AI assistants and autonomous agents may exacerbate the circulation of counterfeit goods by steering consumers toward infringing products.[7]

However, the dual nature of emerging technologies renders them simultaneously a source of the problem and a potential part of the solution. While AI may be weaponized to facilitate IP infringement, it may also be deployed to assist brand owners in the detection, monitoring, and enforcement of their trademark rights.

[7] See, e.g., World Intellectual Property Organization, Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence' (2020) para. 38, https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=499504, arguing that the rise of AI and e-commerce platforms is reshaping the way consumers purchase goods and services, prompting renewed debate about the interaction between AI and trademarks in online environments, and further underscoring that AI-driven interfaces—such as digital assistants, search engines, customer service bots, and online marketplaces—play an increasingly influential role in structuring consumer choice, including by filtering information, limiting brand visibility, and otherwise altering how consumers search for, compare, and select products.

For instance, in recent years, the World Intellectual Property Organization (WIPO) has increasingly leveraged artificial intelligence to enhance efficiency, accuracy, and accessibility across various areas of intellectual property administration. To this end, WIPO has developed and made available a range of AI-powered services and tools designed to support users and stakeholders throughout the IP lifecycle. With specific regard to trademark protection, the Global Brand Database offers an AI-enabled image similarity search function that allows users to upload images or logos and identify identical or visually similar trademarks within the database.[8] This functionality assists practitioners and brand owners in detecting potential trademark infringements and in conducting more comprehensive trademark clearance searches. Similarly, the Vienna Classification Assistant is an AI-driven tool intended to facilitate the application of the Vienna Classification system.[9] By automatically suggesting appropriate Vienna Classification codes for figurative elements of trademarks, the tool enhances both the accuracy and the efficiency of trademark classification processes. In addition, through the Global Goods & Services Terms Explorer, trademark applicants receive assistance in selecting appropriate goods and services terms and their corresponding Nice Classification categories across multiple languages during the filing process.[10] Finally, WIPO is currently developing an additional AI-based tool designed to generate relevant

[8] https://www.wipo.int/en/web/global-brand-database. For a critical analysis of the current state of these techniques, see Julien Cabay, Thomas Vandamme, and Olivier Debeir, 'Looking through the crack in the black box: A comparative case law benchmark for auditing AI-Powered Trade Mark search engines' (2025) 59 Computer Law & Security Review 106167.

[9] https://vienna-assistant.branddb.wipo.int.

[10] https://goods-and-services-assistant.branddb.wipo.int.

keywords to improve the searchability of similar trademarks and to assist applicants in drafting the descriptive elements required in trademark applications.[11]

While AI-powered tools can significantly enhance the efficiency and accuracy of trademark search and clearance processes, they may prove even more effective in the detection of trademark infringement. Traditional methods of monitoring the marketplace for unauthorized uses of trademarks are often time-consuming and resource-intensive. By contrast, AI-driven monitoring systems are capable of continuously scanning the internet to identify potential infringements in near real time. By flagging instances of confusingly similar signs or unauthorized replicas, these tools enable brand owners to take prompt enforcement action and, at the same time, encourage greater engagement by online platforms in the detection and prevention of counterfeit goods.

For example, Deloitte has developed an AI-based tool (Dupe Killer) designed to assist international fashion brands in detecting counterfeit products offered for sale online.[12] Notably, by leveraging machine-learning techniques, the system learns the distinctive shapes and configurations of genuine products and subsequently identifies visually similar items that may constitute copycats. Red Points has developed software that operates not merely as a detection tool, but as a comprehensive enforcement solution designed to prevent copycats from reaching consumers on online marketplaces and social media.[13] Corsearch and MarqVision are other examples of an AI-driven brand protection and trademark intelligence platform whose primary objective is to protect brands from

[11] https://www.wipo.int/en/web/ai-tools-services.

[12] https://www.deloitte.com/uk/en/about/story/impact/dupe-killer-the-attack-on-the-copycats.html.

[13] https://www.redpoints.com/brand-protection-software/.

infringement, counterfeiting, and online abuse at scale.[14] Similarly, MarkMonitor, originally developed by Clarivate, employs machine learning, image recognition, and text analysis to detect infringing content across a wide range of digital environments, including websites, online marketplaces, social media platforms, app stores, and domain names.[15]

In addition, digital platforms have increasingly adopted a proactive approach by leveraging artificial intelligence technologies, including large language models, to detect trademark infringements. A prominent example is Amazon's anti-counterfeiting policy[16], under which the company has launched Project Zero[17], established the Brand Registry[18], created a dedicated Counterfeit Crimes Unit, publishes an annual Brand Protection

[14] https://corsearch.com; https://www.marqvision.com.

[15] https://www.markmonitor.com.

[16] Amazon, 'How Amazon uses AI innovations to stop fraud and counterfeits' (2025) https://www.aboutamazon.com/news/policy-new-views/amazon-brand-protection-report-2024-counterfeit-products.

[17] https://sell.amazon.it/en/brand-registry/project-zero?mons_sel_locale=en_GB. See also Daniel Seng, 'Detecting and Prosecuting IP Infringement with AI: Can the AI Genie Repulse the Forty Counterfeit Thieves of Alibaba?', in Jyh-An Lee, Reto Hilty, and Kung-Chung Liu (eds), *Artificial Intelligence and Intellectual Property* (Oxford:Oxford University Press, 2021) 292; Dev S. Gangjee, 'A Quotidian Revolution: Artificial Intelligence and Trade Mark Law', in Ryan Abbott (ed), *Research Handbook on Intellectual Property and Artificial Intelligence* (Cheltenham:Edward Elgar Publishing, 2022) 325.

[18] https://sell.amazon.it/en/brand-registry#protect.

Report, and actively cooperates with brand owners in enforcement actions against counterfeiters.[19]

The present contribution focuses specifically on the extent to which AI-powered enforcement mechanisms may shape the future framework of online intermediaries' liability in the field of trademark protection. Indeed, owing to the pronounced structural asymmetries between brand owners and digital intermediaries, the latter are uniquely positioned to address the widespread phenomenon of counterfeiting in a more effective and systematic manner. Against this background, AI tools may help overcome the structural and informational asymmetries between brand owners and online platforms by automating monitoring and enforcement processes that would otherwise be prohibitively costly, slow, or fragmented. As a result, the deployment of AI technologies by online platforms may both strengthen *ex post* enforcement—by automatically triggering the removal of illegal listings under established notice-and-takedown mechanisms—and enable *ex ante* intervention, by preventing, or at least significantly reducing, the likelihood that unauthorized replicas reach the market and attract consumers' attention in the first place.

For these reasons, it may be argued that the rise of AI and the advent of the algorithmic age mark a paradigm shift in trademark enforcement. In this emerging framework, enforcement is likely to rely increasingly on an architecture of defense by design

[19] See, e.g., Amazon, 'Amazon takes legal action against massive trademark fraud scheme' (2025) https://www.aboutamazon.com/news/policy-news-views/amazon-counterfeit-crimes-unit-latest-updates-2024; Prada, 'Prada Group and Amazon Together Against International Counterfeit' (2023) https://www.pradagroup.com/en/news-media/news-section/23-10-23-prada-group-amazon.html.

implemented by online intermediaries, rather than primarily on traditional judicial mechanisms.[20]

The paper is structured as follows. Section 2 illustrates the current U.S. and EU frameworks governing online intermediary liability, drawing on both relevant case law and most recent regulatory initiatives. Section 3 examines the implications of AI-enabled tools, outlining both their potential and the challenges and opportunities they present for trademark enforcement in digital markets. Section 4 concludes.

2. The current framework governing online intermediary liability

The current regulatory framework emerged in response to the rise of internet and reflects the central role played by internet service providers (ISPs) as key channels for intellectual property infringement, particularly in the field of copyright protection.

In this context, alongside the traditional rules addressing both primary (direct) and secondary (indirect) liability, both the U.S. and the EU developed a specific regulatory architecture for online intermediaries. In particular, under the 1998 U.S. Digital Millennium Copyright Act (DMCA)[21] and the 2000 EU e-Commerce Directive[22], the liability of Internet service providers (ISPs) for illegal activities carried out through their services is structured around a system of safe harbours, differentiated according to the

[20] See, e.g., Maria Lucia Passador, 'Algorithmic Couture: Trademark Protection in the AI Era' (2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5311228.

[21] 17 U.S. Code §512.

[22] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), [2000] OJ L 178/1.

type of intermediary involved, but fundamentally grounded in the premise that service providers enjoy immunity insofar as they perform a merely passive role. For intermediaries most directly exposed to IP infringements (i.e., hosting providers), liability is excluded where they lack actual knowledge of illegal activity or, upon acquiring such knowledge or awareness, act expeditiously to remove or disable access to the unlawful content through the so-called notice-and-takedown procedure.

At the same time, as a general principle common to both the U.S. and EU frameworks, ISPs are not subject to a general obligation to monitor the information they transmit or store, nor to a general duty to actively seek out facts or circumstances indicating the presence of illegal activities on their platforms.

In the field of trademark law a particularly prominent role is played by search engines and online marketplaces, especially through their keyword advertising services, which have been the subject of extensive litigation concerning the legality of selecting trademarks as advertising keywords.[23] In order to increase the likelihood that a given advertisement is displayed to users, advertisers may have an incentive to bid on keywords corresponding to trademarks, including those of competitors. Conversely, trademark proprietors have challenged—often against both advertisers and online intermediaries—the practice of using a competitor's mark to trigger the display of sponsored links, arguing that such use may adversely affect the essential functions of the trademark, including its origin and advertising functions.

[23] See, e.g., Giuseppe Colangelo, 'Competing through keyword advertising' (2020) 16 Journal of Competition Law & Economics 306.

Against this background, the EU and US case law offered important insights to clarify the boundaries of ISPs' liability.

In *Google France v. Louis Vuitton*[24] and *L'Oréal v. eBay*[25], the European Court of Justice (ECJ) held that, once the existence of unlawful activity carried out by a third party using the services of an intermediary is established, the intermediary is exempt from liability provided that its conduct is confined to a merely technical, automatic, and passive role. By contrast, where the intermediary is found to exercise control over the unlawful information, it cannot benefit from the safe-harbour regime and may be held liable on account of its active involvement. In this respect, the Court clarified that an intermediary plays an active role where it provides assistance to trademark infringers, for instance by optimizing or promoting the presentation of counterfeit goods. Moreover, the ECJ specified that even an intermediary that has not played an active role may nonetheless lose the benefit of the safe harbour if it is aware of facts or circumstances from which a diligent economic operator should have inferred the existence of illegal activity and, despite such awareness, fails to act expeditiously to prevent its continuation, whether by removing the infringing material or by disabling access to the users responsible for its dissemination.

On the U.S. side, the general principles governing secondary liability in trademark cases were articulated by the Supreme Court in a non-digital context in *Inwood Laboratories*.[26] The Court held that a manufacturer or distributor may be held contributorily liable for

[24] ECJ, 23 March 2010, Joined Cases C-236/08, C-237/08 and C-238/08, *Google France SARL v. Louis Vuitton Mallettier SA and others,* EU:C:2010:159.

[25] ECJ, 18 June 2009, Case C-487/07, *L'Oréal SA and others v. Bellure NV and others*, EU:C:2009:378.

[26] *Inwood Laboratories v. Ives Laboratories*, 456 U.S. 844 (1982).

trademark infringement where it intentionally induces another party to infringe a trademark, or where it continues to supply its product to a party whom it knows, or has reason to know, is engaging in trademark infringement. In such circumstances, the manufacturer or distributor may be held responsible for the harm resulting from the infringing conduct.

Applying this two-part test in the digital environment, in *Tiffany v. eBay* the Second Circuit rejected a contributory infringement claim reiterating that, to satisfy the *Inwood* test, it is not enough to have general knowledge as to counterfeiting on its website to impose upon eBay an affirmative duty to remedy the problem. Rather, the defendant must supply its product or service to identified individuals that it knows or has reason to know are engaging in trademark infringement. However, a service provider is not permitted willful blindness. Hence, contributory liability may arise if eBay had reason to suspect that counterfeit Tiffany goods were being sold through its website, and intentionally shielded itself from discovering the offending listings or the identity of the sellers behind them. In this regard, efforts undertaken by eBay were relevant for inducing the Court to dismiss the charges. Indeed, eBay implemented, among other things, a fraud engine dedicated to ferreting out illegal listings and employed manual searches for keywords in listings in an effort to identify blatant instances of potentially infringing activity. Moreover, unlike the approach adopted by the ECJ, U.S. courts have held that an ISP's use of trademarks as advertising keywords constitutes use in commerce, thereby opening

the door to direct infringement claims against online intermediaries where such use gives rise to a likelihood of consumer confusion.[27]

However, following more recent developments in the case law on copyright about the active role of ISPs[28], the ECJ has also acknowledged the possibility of direct liability of digital intermediaries under trademark law arising from users' unlawful activities, notably in cases involving the availability of third-party listings for infringing goods. Notably, in *Louboutin v. Amazon*, the Court emphasized the relevance of both the platform's business model and consumers' perceptions. It held that an online marketplace operator may be directly liable for trademark infringement where a reasonably well-informed and observant user establishes a link between the operator's services and the trademark at issue.[29] Such a link may arise, in particular, where, in light of all the relevant circumstances, users may gain the impression that the platform operator itself is marketing the goods bearing the sign, in its own name and on its own account. According to the ECJ, this assessment requires consideration of a range of factors, including the operator's use of a uniform presentation format for offers published on its website (covering both goods sold by the operator itself and goods offered by third-party sellers), the prominent display of the operator's logo as a well-known distributor on those listings, and the provision of ancillary services to third-party sellers, such as the storage and shipping of goods bearing the contested sign.

---

[27] See, e.g., *Rescuecom v. Google*, 562 F.3d 123 (2nd Cir. 2009); *Playboy Enterprises v. Netscape Comm*., 354 F.3d 1020 (9th Cir. 2004).

[28] See, e.g., ECJ, 22 June 2021, Joined Cases C-682/18 and C-683/18, *Frank Peterson v. YouTube* and *Elesevier v. Cyando,* EU:C:2021:503.

[29] ECJ, 22 December 2022, Joined Cases C-148/21 and C-184/21, *Louboutin v. Amazon,* EU:C:2022:1016.

Finally, the recently enacted Digital Services Act (DSA), adopted in response to the growing challenges posed by illegal content (including counterfeit goods) in the digital environment, introduces additional obligations and responsibilities for online platforms within the European regulatory framework.[30] Indeed, with the aim of strengthening the ability of trademark owners to enforce their rights online, reducing the prevalence of counterfeit goods, and enhancing platform accountability, while preserving the traditional safe-harbour framework, the DSA supplements the e-commerce Directive by introducing a set of reinforced obligations that vary according to the size, role, and societal impact of intermediary service providers. Although all intermediary service providers are required to ensure that any restrictions imposed through content moderation duly respect the rights and legitimate interests of all parties, the majority of content moderation related obligations apply specifically to online platforms, online marketplaces, designated very large online platforms (VLOPs), and very large online search engines (VLOSEs).

Notably, providers of online platforms—defined as hosting services that, at the request of a recipient, store and disseminate information to the public—are required, *inter alia*, to provide effective redress mechanisms for users, to prioritize notices submitted by trusted flaggers, to adopt measures against abusive notices and counter-notices, and to comply with a range of transparency obligations. Providers of online marketplaces are required to carry out 'Know Your Business Customer' (KYBC) checks on traders offering products or services to consumers, including the verification of information supplied by traders through reliable and independent sources. VLOPs and VLOSEs are also required

[30] Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

to carry out annual assessments of the systemic risks arising from the functioning and use of their services and to mitigate the risks identified through the implementation of tailored, reasonable, proportionate, and effective measures. They are required to take specific actions in the event of a crisis, to submit to annual independent audits verifying compliance with the obligations set out in the DSA, and to provide access to data necessary for monitoring such compliance.

3. Algorithmic trademark enforcement: the progressive erosion of the principle of no general monitoring obligation

The integration of AI into trademark law and practice is expected to significantly reshape the regulatory enforcement landscape outlined above, by delivering advantages that markedly enhance the efficiency, accuracy, and overall effectiveness of trademark enforcement and administration. In digital environments characterized by scale, speed, and cross-border fragmentation, traditional enforcement mechanisms—largely dependent on *ex post* interventions—have increasingly proven inadequate. AI-based tools respond to these structural limitations by enabling a more systematic, data-driven, and proactive approach to trademark protection.

In particular, AI systems are capable of identifying complex and evolving patterns of trademark infringement that are difficult to detect through traditional, predominantly manual approaches. Whereas conventional enforcement relies heavily on human interpretation and labor-intensive searches—often constrained by errors, resource limitations, and problems of scale—AI can process and correlate vast datasets across multiple platforms and jurisdictions. Through techniques such as machine learning, computer vision, and natural language processing, AI systems are able to detect subtle

forms of brand misuse, including minor variations in logos, trade dress, product names, or descriptive language deliberately designed to evade detection. This capacity is especially relevant in the context of counterfeiting and parasitic practices, where infringers continuously adapt their strategies in response to enforcement efforts. Moreover, AI-driven tools enable continuous and near real-time monitoring of online platforms, automating the detection of trademark infringements and allowing for faster and more effective enforcement responses. By providing timely alerts and prioritizing high-risk infringements, AI tools facilitate prompt intervention through notice-and-takedown procedures, negotiated settlements, or other platform-based enforcement mechanisms, thereby reducing both the scale and duration of harm. Finally, by managing large volumes of data across platforms, channels, and jurisdictions, AI significantly enhances the scalability of trademark enforcement. It enables brand owners and intermediaries to move beyond isolated, case-by-case actions and to adopt a more strategic and systemic perspective, identifying recurring infringement patterns, organized networks of counterfeiters, and emerging risks.

More specifically, with regard to the underlying technologies that underpin AI-based tools, machine learning algorithms play a central role in trademark enforcement by enabling the automated identification of potential infringements. These systems are trained on curated datasets comprising both infringing and non-infringing product listings, allowing the models to learn the patterns and features that distinguish unlawful uses of trademarks from legitimate ones. Once deployed, the models can operate in real time or in batch-processing modes, systematically analyzing product names, descriptions, images, and seller-related data to identify suspicious listings. By detecting trademark-related keywords, visual similarities, and other relevant risk signals, machine learning

enables scalable, continuous, and increasingly accurate enforcement across digital marketplaces.

Natural language processing (NLP) techniques constitute a further core component of AI-based trademark enforcement, particularly in the analysis of textual data such as product descriptions, titles, reviews, and metadata. By transforming unstructured text into structured and machine-readable information, NLP enables more accurate categorization, comparison, and assessment of online listings. In the enforcement context, NLP algorithms can process large volumes of textual content to identify suspicious keywords, linguistic patterns, and semantic anomalies commonly associated with counterfeit or infringing products. By flagging such risk indicators at scale, NLP supports the early detection of potential infringements and enables more proactive and targeted anti-counterfeiting interventions.

Moreover, the detection of counterfeit goods can be significantly enhanced through the application of computer vision technologies, which analyze product images to identify visual similarities or anomalies indicative of counterfeiting. By leveraging machine learning techniques, computer vision systems can process large volumes of images and compare them against reference images of authentic products. This enables the identification of potential counterfeits on the basis of visual cues such as design features, logos, packaging, and overall appearance. In addition, computer vision tools can support the tracking and monitoring of counterfeit distribution patterns across platforms and geographic regions, thereby contributing to more systematic and coordinated enforcement efforts.

Taken together, this technological toolkit has enabled AI-based solutions to emerge as powerful instruments for combating counterfeiting and trademark infringement on digital

platforms. Therefore, as emphasized in recent scholarship, AI has moved beyond a merely supportive role and now constitutes a central pillar of contemporary trademark enforcement.[31] This development entails not only the adoption of increasingly sophisticated technological tools, but also a deeper reconceptualization of brand protection as a systemic and anticipatory process. Indeed, in digital ecosystems where trademarks can be easily replicated and strategically manipulated, enforcement can no longer rely primarily on *ex post* judicial intervention. Rather, AI enables the development of preventive, architecture-based mechanisms that enhance traceability, distribute enforcement intelligence across platforms, and embed legal safeguards directly into market design. As a result, trademark protection is progressively shifting from reactive detection toward proactive control, redefining enforcement as an integral component of digital governance rather than a predominantly courtroom-centered activity.[32]

In response to increasing pressure on online platforms to play a more active role in preventing and promptly removing infringing offerings, many—particularly online marketplaces—have adopted such a proactive stance by implementing anti-counterfeiting policies based on AI-driven filtering and monitoring technologies, while also promoting close cooperation with brand owners.

This development has significant practical implications for the future regulatory landscape of digital markets. Although the principle prohibiting a general monitoring

[31] Passador (n 20). See also Pokrovskaya Anna Vladimirovna, 'The application of AI technologies: Enforcement of trademark rights on e-commerce marketplaces' (2025) 28 Journal of World Intellectual Property 665; Dev S. Gangjee, 'Panoptic Brand Protection? Algorithmic Ascendancy in Online Marketplaces' (2024) 46 European Intellectual Property Review 448.

[32] Passador (n 20).

obligation formally remains in force, the growing deployment of AI technologies together with the expansion of regulatory obligations imposed on online platforms suggests, *de facto*, a markedly different enforcement paradigm.

From this perspective, the evolution of algorithmic enforcement in the trademark field increasingly mirrors regulatory approaches developed in the area of copyright.[33] A comparable paradigm shift has been expressly promoted in copyright law through Article 17 of the Directive on Copyright in the Digital Single Market.[34] Under this provision, online content-sharing service providers may avoid direct liability for infringing works uploaded by users only if they demonstrate that they have made best efforts to obtain authorization for such content and to ensure, in accordance with high industry standards of professional diligence, to ensure the unavailability of unauthorized works on their services. Compliance with these obligations has, in practice, led platforms to adopt preventive measures such as automated content filtering, relying on algorithmic systems to block the upload of unlawful material.

Admittedly, this provision has proven highly controversial and has sparked intense debate regarding its compatibility with fundamental rights, particularly in light of the significant

[33] In a similar vein, see, e.g., João Pedro Quintais, 'A new liability paradigm for online platforms in EU copyright law', in Katja Weckström, Maria Lillà Montagnani, and Katarzyna Klafkowska-Waśniowska (eds) *Governance of Digital Single Market Actors* (Cheltenham:Edward Elgar Publishing, 2025) 172.

[34] Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.

risks it poses to freedom of expression and information.[35] The need to balance these competing interests has also prompted specific intervention by the ECJ, which has sought to delineate the limits within which such preventive enforcement mechanisms may operate consistently with fundamental rights protections.[36]

At the same time, it may be acknowledged that, in the trademark context, the risk of disproportionately restricting fundamental rights is lower, and the associated balancing exercise is therefore less complex than in the field of copyright. Moreover, as noted in the literature, the DSA, with its emphasis on algorithmic transparency, accountability, and systemic risk assessment, offers a potential framework for reconciling technological innovation with the protection of fundamental rights.[37]

After all, the deployment of AI technologies inevitably entails managing complex trade-offs: while automated enforcement can significantly enhance efficiency and effectiveness, it may at the same time raise concerns relating to due process, accuracy, and accountability.

---

[35] See, e.g., Christophe Geiger and Bernd Justin Jütte, 'Platform Liability under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70 GRUR International 517.

[36] ECJ, 26 April 2022, Case C-401/19, *Republic of Poland v. European Parliament*, EU:C:2022:297.

[37] See, e.g., Giancarlo Frosio, 'Algorithmic Enforcement Tools: Governing Opacity with Due Process' in Simona Francese and Roberto King (eds), *Driving Forensic Innovation in the 21st Century: Crossing the Valley of Death* (Cham:Springer International Publishing, 2024) 195; Gangjee (n 31). See also Christina Angelopoulos and Martin Senftleben, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022.

4. Concluding remarks

Since the advent of the internet, one of the central themes in the debate on intellectual property protection has been the pivotal role played by online intermediaries. Acting as the main gateways to end users, these actors have progressively been subject to expanding regulatory and enforcement obligations. This development has been accompanied by growing skepticism regarding the effectiveness of traditional *ex post* judicial enforcement mechanisms.

As a result, a twofold paradigm shift has gradually emerged. First, online intermediaries are increasingly required to adopt a proactive approach to infringement detection, deploying measures aimed not only at the prompt removal of illegal content or goods, but also at preventing infringements from occurring in the first place. Second, enforcement responsibilities have progressively shifted from public authorities toward private actors.

Against this backdrop, the advent of AI represents the latest stage in this broader evolutionary trajectory. As with other disruptive technologies, artificial intelligence simultaneously generates significant opportunities and substantial risks, and may therefore function both as a source of new challenges and as a means of addressing them. In the trademark context, the growing deployment of AI may facilitate novel forms of infringing conduct, enabling more sophisticated, scalable, and evasive counterfeiting practices. At the same time, however, these very technologies provide increasingly powerful instruments for trademark enforcement, enhancing the ability to prevent, detect, and monitor the dissemination of counterfeit goods across digital markets.

The dual and ambivalent nature of algorithmic enforcement is not confined to the trademark domain. In the field of competition law, for instance, an increasing number of firms have adopted algorithms for dynamic pricing, enabling prices to be automatically adjusted in response to changing market conditions, including competitors' pricing strategies.[38] The widespread use of algorithmic pricing has consequently raised concerns about its potential to facilitate not only traditional forms of collusion, but also novel modes of coordination, insofar as algorithms may interact and coordinate independently of human intervention and may even learn to collude autonomously. At the same time, artificial intelligence may also serve as a valuable instrument for antitrust enforcement.[39] In particular, its capacity to process vast datasets and identify complex patterns creates significant opportunities for competition authorities, which may increasingly rely on algorithmic and AI-driven analytical tools in the detection and investigation of anticompetitive conduct.

While this dual character underscores the need for a nuanced regulatory approach capable of harnessing the enforcement potential of AI while mitigating its associated risks, it also serves as a reminder that, in the age of AI, policymakers are inevitably required to navigate challenging trade-offs and to operate in an environment marked by heightened uncertainty and risk.

---

[38] Stephanie Assad, Robert Clark, Daniel Ershov, and Lei Xu, 'Algorithmic Pricing and Competition: Empirical Evidence from the German Retail Gasoline Market' (2024) 132 Journal of Political Economy 723.

[39] See, e.g., European Commission, 'White Paper on Artificial Intelligence: A European approach to excellence and trust' COM(2020) 65 final, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.