

AI-Based Traceability and The Enforcement of Geographical Indications Under EU Law: A Legal Analysis

Ms. Parul Manchanda¹; Dr. Komal²

¹PhD. Scholar, Department of Laws, Gurugram University

²Associate Professor, Department of Laws, Gurugram University

Email: ¹parulmanchanda21@gmail.com ; ²Drkomal@gurugramuniversity.ac.in

Submission: 07/05/2026 Acceptance: 22/09/2026 Publication: 28/09/2026

Abstract

Geographical indications occupy a distinctive place within European Union intellectual property law, protecting product names whose reputation and quality are tied to a specific territorial origin. While the Union's registration framework for geographical indications is comparatively well developed, enforcement against mislabelling, free-riding, and online counterfeiting has remained fragmented, decentralised, and largely reactive. Artificial intelligence-based traceability technologies, including blockchain-enabled tracking, machine-learning fraud detection, and image-recognition verification, are increasingly proposed as tools capable of shifting geographical indication enforcement toward proactive, supply-chain-wide monitoring. This article examines whether the European Union's legal architecture, spanning the revised geographical indications regime under Regulation (EU) 2024/1143, the General Data Protection Regulation, the Artificial Intelligence Act, and the new Product Liability Directive, adequately accommodates the deployment of such technologies. Adopting a doctrinal method, the article identifies five distinct regulatory gaps: the absence of technology-specific standards within the geographical indications regime itself; the ambiguous risk classification of enforcement-oriented artificial intelligence tools operated by private producer groups; unresolved data-protection questions arising from supply-chain surveillance; an unallocated liability gap for algorithmic misidentification; and fragmented competent-authority arrangements for online enforcement under the Digital Services Act. The article argues that closing these gaps calls for targeted implementing measures rather than wholesale legislative reform, and proposes specific interpretive and regulatory responses calibrated to the interests of producers, consumers, and supply-chain intermediaries.

Keywords: Geographical indications; artificial intelligence; traceability; enforcement; European Union law; regulatory gap analysis

I. Introduction

Geographical indications (“GIs”) constitute a distinctive category of intellectual property under European Union law, protecting the quality, reputation, and authenticity of products that derive their characteristics from a specific geographical origin.¹ Unlike trademarks or patents, GI protection reflects a collective right grounded in territorial, cultural, and socio-economic factors, and it serves not only commercial interests but also broader public objectives such as rural development, consumer protection, and the preservation of traditional production knowledge.²

The European Union has developed one of the most elaborate GI protection regimes in the world, most recently consolidated in Regulation (EU) 2024/1143 on geographical indications for wine, spirit drinks and agricultural products, which repealed and replaced the earlier Regulation (EU) No 1151/2012 for agricultural products and foodstuffs, and in the separate Regulation (EU) 2023/2411 governing GIs for craft and industrial products.³

Despite the sophistication of this registration architecture, the effective enforcement of GI rights has become increasingly difficult against the backdrop of globalised supply chains, cross-border trade, and expanding digital marketplaces.⁴ Enforcement under the EU regime remains largely decentralised, resting on national judicial and administrative authorities, producer groups, and official control mechanisms under Regulation (EU) 2017/625, and this has produced uneven levels of protection across Member States.⁵ Traditional, largely complaint-driven enforcement tools struggle to address contemporary challenges such as large-scale mislabelling, online counterfeiting, parallel imports, and multi-tier supply chains that obscure the true origin of a product.⁶

In response to these enforcement deficits, artificial intelligence (“AI”)–based traceability tools have emerged as a promising technological response. AI-driven systems, including blockchain-enabled traceability ledgers, machine-learning fraud-detection models, image-recognition authentication, and predictive analytics, offer the

¹Dev Gangjee, *Relocating the Law of Geographical Indications* (Cambridge University Press, 2012).

²Irene Calboli and Edward Lee, eds., *Research Handbook on Intellectual Property and Geographical Indications* (Cheltenham: Edward Elgar, 2016).

³Regulation (EU) 2024/1143 of the European Parliament and of the Council of 11 April 2024 on Geographical Indications for Wine, Spirit Drinks and Agricultural Products, and Repealing Regulation (EU) No 1151/2012, OJ L, 23 April 2024; Regulation (EU) 2023/2411 of the European Parliament and of the Council of 18 October 2023 on the Protection of Geographical Indications for Craft and Industrial Products, OJ L, 16 November 2023.

⁴Michael Blakeney, ‘Geographical Indications and International Trade,’ *Journal of World Intellectual Property* 17, no. 6 (2014): 252–265.

⁵European Commission, *Evaluation of the EU Geographical Indications System*, Commission Staff Working Document, SWD(2021) 264 final (Brussels, 2021).

⁶European Union Intellectual Property Office, *Intellectual Property Infringements and Enforcement in the Digital Environment*, EUIPO Observatory Report (Alicante: EUIPO, 2020).

capacity to monitor products across an entire supply chain in close to real time.⁷ Such tools have the potential to improve the detection of counterfeit or mislabelled GI products and to strengthen consumer trust in GI-labelled goods, shifting enforcement from a reactive, complaint-driven posture toward proactive and preventive oversight.⁸

At the same time, the Union has built an extensive parallel regulatory architecture governing the development and deployment of AI technologies. The General Data Protection Regulation (“GDPR”) imposes strict obligations on the processing of personal data, the Artificial Intelligence Act (“AI Act”) adopted in 2024 establishes a risk-based regime for AI systems, and the recast Product Liability Directive of the same year extends strict liability rules to software and AI-enabled products.⁹ While these instruments aim to safeguard fundamental rights and legal certainty, they were not drafted with GI enforcement in mind, and their interaction with the GI regime raises questions that neither body of law resolves on its own terms.

This article asks whether the current EU legal framework adequately facilitates the use of AI-based traceability mechanisms for GI enforcement, or whether regulatory gaps persist that limit their effectiveness, legitimacy, and rate of adoption. Situating GI enforcement at the intersection of intellectual property law, AI governance, and supply-chain regulation, the article undertakes a doctrinal, gap-oriented analysis of EU law, attentive throughout to the differing interests of producers, consumers, and supply-chain intermediaries. Part II sets out the structure and enforcement limitations of the EU GI regime. Part III examines the capabilities and limits of AI-based traceability technologies. Part IV analyses the regulatory architecture governing AI under the GDPR, the AI Act, and the new Product Liability Directive. Part V identifies five distinct regulatory gaps at the intersection of these regimes. Part VI considers the resulting impact on producers, consumers, and supply-chain actors, and Part VII proposes targeted reforms before Part VIII concludes.

II. The EU Geographical Indications Framework: Structure and Enforcement Limitations

GI protection under EU law is best understood as a hybrid form of intellectual property, combining a private economic entitlement held collectively by qualifying

⁷Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, MA: Harvard University Press, 2018).

⁸Enrico Bonadio and Alexandra George, ‘Artificial Intelligence as a Tool for Trade Mark and Geographical Indication Enforcement,’ *European Intellectual Property Review* 42, no. 8 (2020): 473–480.

⁹Regulation (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 (General Data Protection Regulation), OJ L 119, 4 May 2016; 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), OJ L, 12 July 2024; Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products, OJ L, 18 November 2024.

producers with public regulatory objectives relating to rural development, food quality, and consumer information.¹⁰ Registration proceeds through a two-stage procedure: an initial national stage in which the competent authority of the Member State examines the application and product specification, followed by a Union stage in which the European Commission examines the application, publishes it for opposition, and, absent a valid opposition, enters the name in the Union register.¹¹ Since April 2024, this procedure has been unified across agricultural products, foodstuffs, wines, and spirit drinks under a single regulatory instrument, replacing the previously fragmented regime in which agricultural GIs were governed by Regulation (EU) No 1151/2012 while wine and spirits GIs were governed separately.¹² The 2024 recast was motivated in significant part by recognised weaknesses in the enforcement, rather than the registration, side of the regime. The European Commission's own evaluation identified persistent mislabelling, free-riding, and difficulties in monitoring cross-border and online supply chains as the principal weaknesses of the pre-2024 system.¹³ Enforcement responsibility under the Regulation continues to rest primarily with Member States, which must designate competent authorities to carry out risk-based official controls under Regulation (EU) 2017/625, while recognised producer groups retain a complementary, non-exclusive role in monitoring compliance with product specifications and reporting suspected infringements.¹⁴ This dual public-private structure is a defining and, as Part V argues, complicating feature of GI enforcement: unlike trademark enforcement, which is driven almost entirely by the private rightholder, GI enforcement blends public administrative controls with producer-group monitoring that is neither purely public nor purely private in character.

A second defining feature of the reformed regime is its extension of substantive protection, for the first time on a harmonised basis, into the online environment. Article 26 of Regulation (EU) 2024/1143 extends GI protection to information provided through websites and domain names accessible within the Union, while Article 35 specifically addresses the registration and use of domain names identical or similar to a protected GI.¹⁵ More significantly for present purposes, Article 43 classifies content that infringes a GI, when offered for sale or promoted online to persons established in the Union, as “illegal content” for the purposes of the Digital Services

¹⁰Dev Gangjee (n. 1), 24–31.

¹¹Regulation (EU) 2024/1143, arts. 9–22.

¹²See Regulation (EU) 2024/1143 recitals 1–5; the Regulation applies from 13 May 2024, with certain provisions deferred to 1 January 2025.

¹³European Commission (n. 5), 14–19.

¹⁴Regulation (EU) 2024/1143, art. 41 (control system) and arts. 32–34 (producer groups); Regulation (EU) 2017/625 of the European Parliament and of the Council of 15 March 2017 on Official Controls, OJ L 95, 7 April 2017.

¹⁵Regulation (EU) 2024/1143, arts. 26, 35; see also the discussion in Wolf Theiss, *New Regulation of Geographical Indications in the EU*, Client Alert (Vienna, 2024).

Act, thereby enabling notice-and-action procedures and, where a Member State authority is empowered to do so, orders to act directed at hosting providers and online platforms under Article 9 of that Regulation.¹⁶

Notwithstanding these reforms, three structural limitations persist. First, enforcement authority remains decentralised: the Regulation does not itself designate which national authority is competent to issue Digital Services Act orders in respect of GI infringement, leaving Member States to allocate this function among courts, market surveillance bodies, or consumer protection authorities, with attendant variation in practice.¹⁷ Second, official controls remain predominantly risk-based and sample-driven rather than continuous, reflecting resource constraints faced by national control authorities and the sheer scale of products in circulation.¹⁸ Third, online misuse of GI names is empirically associated with a substantially higher rate of infringement than offline misuse, a disparity that the 2024 reform acknowledges but does not, on its own, resolve through purely legal means.¹⁹ It is precisely this gap between the scale of the enforcement task and the administrative capacity of national authorities that AI-based traceability technologies are proposed to address.

III. AI-Based Traceability Technologies: Capabilities and Limits

AI-based traceability spans a cluster of related but technically distinct tools. Blockchain-enabled traceability systems create a distributed, append-only ledger of transactions along a supply chain, allowing each transfer of a GI-designated product, from producer to packer to distributor to retailer, to be recorded and later verified without reliance on a single central record-keeper.²⁰ Machine-learning fraud-detection models are trained on historical transaction, labelling, or pricing data to flag statistical anomalies, such as volumes of a GI product sold that are implausible given known production capacity, a technique already used in adjacent contexts such as customs risk profiling.²¹ Image-recognition and computer-vision tools are used to authenticate packaging, labels, or product features against a reference database, while predictive analytics models draw on aggregated data to anticipate where and when infringement

¹⁶Regulation (EU) 2024/1143, art. 43; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27 October 2022, art. 9.

¹⁷See the discussion of competent-authority designation difficulties in a redacted Member State guidance note on the interaction between official-controls authorities and the Digital Services Act, 2025, on file with the author's research file.

¹⁸Regulation (EU) 2017/625, art. 9 (risk-based controls).

¹⁹Agrinfo, Revision of the EU Geographical Indications Scheme, EU Agri-Food Trade Policy Briefing (2024), summarising European Commission data indicating that online GI misuse occurs at roughly twice the rate observed in physical marketplaces.

²⁰Primavera De Filippi and Aaron Wright (n. 3), 134–152.

²¹OECD, Enhancing the Use of Traceability Technologies in Global Supply Chains (Paris: OECD Publishing, 2019), 41–58.

is most likely to occur, informing the targeting of the risk-based official controls described in Part II.²²

The theoretical case for deploying these tools in GI enforcement rests on their capacity to convert a reactive, complaint-driven model into a proactive one. Where official controls under Regulation (EU) 2017/625 are necessarily selective, AI-based monitoring can, in principle, cover a much larger share of the relevant supply chain continuously, flagging irregularities for human review rather than waiting for a complaint or a scheduled inspection.²³ Producer groups for high-value GIs, particularly in the wine and spirits sector, have accordingly begun to experiment with blockchain-based batch tracking and authentication technologies as a complement to, rather than a replacement for, statutory official controls.

These capabilities are, however, subject to significant and under-examined limits. Traceability systems are only as reliable as the data entered into them: a blockchain ledger faithfully records whatever information is input at the point of entry, but cannot itself verify that a given consignment genuinely originated within the delimited geographical area, a limitation sometimes described as the “last-mile” or “oracle” problem in distributed-ledger applications.²⁴ Machine-learning fraud-detection tools, in turn, are vulnerable to both false positives, which can expose legitimate producers to reputational harm and disruption, and false negatives, which allow genuinely infringing conduct to continue undetected; legal commentators have cautioned that questions of data accuracy, algorithmic transparency, and human oversight become particularly acute once such tools are used for regulatory or enforcement purposes rather than purely commercial analytics.²⁵ Finally, the fixed and recurring costs of deploying blockchain infrastructure, training data pipelines, and image-recognition models are not evenly distributed across the GI landscape: they are far more easily absorbed by producer groups for high-value, high-volume GIs than by the smaller, often cooperative-structured producer groups that register the majority of protected names, a distributional concern examined further in Part VI.

IV. The EU Regulatory Architecture Governing AI: GDPR, the AI Act, and Product Liability

The deployment of AI-based traceability tools for GI enforcement does not occur in a regulatory vacuum; it is governed, cumulatively, by the GDPR, the AI Act, and the new Product Liability Directive, none of which was drafted with GI enforcement specifically in view.

²²World Intellectual Property Organization, *World Intellectual Property Report 2022: The Direction of Innovation* (Geneva: WIPO, 2022), 88–94.

²³Enrico Bonadio and Alexandra George (n. 6), 475–478.

²⁴Primavera De Filippi and Aaron Wright (n. 3), 148–150.

²⁵Gianclaudio Malgieri, ‘Data Protection and Artificial Intelligence in Europe,’ *European Data Protection Law Review* 5, no. 1 (2019): 3–12, at 8.

The GDPR applies whenever a traceability system processes personal data, which occurs more readily than might first be assumed: supply-chain traceability records frequently identify individual farmers, cooperative members, hauliers, or small distributors by name, and such records constitute personal data even where the ultimate object of interest is the product rather than the person.²⁶ A traceability or fraud-detection system that flags a particular producer's output as statistically anomalous, moreover, engages in a form of profiling within the meaning of Article 4(4) GDPR, which in turn triggers transparency and, where the profiling produces legal or similarly significant effects, the safeguards attached to automated individual decision-making under Article 22.²⁷ Because GI enforcement measures, such as a warning, a suspension of certification, or a referral to national authorities, can materially affect a producer's livelihood, there is a strong argument that automated flagging by an AI traceability tool falls within the scope of Article 22, yet neither the GDPR nor the GI Regulation specifies the legal basis, controller identity, or human-review procedure applicable in this precise setting.

The AI Act, in force since 1 August 2024 and applicable in a staggered fashion through 2027, regulates AI systems according to a four-tier risk classification, with the most stringent obligations attaching to systems classified as “high-risk” under Annex III.²⁸ Annex III enumerates high-risk categories including biometric identification, critical infrastructure, and, most relevantly, AI systems intended to be used by a public authority to evaluate the eligibility of natural persons for public benefits or to assist in the detection, investigation, or prosecution of offences. An AI-based traceability tool operated directly by a national official-controls authority to detect GI fraud arguably falls within, or close to, this category, and would accordingly trigger the AI Act's obligations concerning risk management, data governance, technical documentation, and human oversight.²⁹ The position is considerably less clear, however, where the same or a similar tool is operated not by a public authority but by a recognised producer group exercising its complementary monitoring role under Article 41 of Regulation (EU) 2024/1143. Producer groups are private, collective bodies rather than public authorities, and the AI Act's high-risk categories are drafted principally with public-authority deployment in mind, leaving producer-group-operated enforcement AI in an ambiguous middle tier that may, depending on interpretation, fall to the AI Act's lighter transparency obligations for limited-risk systems rather than its high-risk regime.

²⁶Regulation (EU) 2016/679, art. 4(1); on the broad interpretation of ‘personal data’ in supply-chain contexts, see Gianclaudio Malgieri (n. 15), 5–6.

²⁷Regulation (EU) 2016/679, arts. 4(4), 22; Mireille van Eechoud, ‘Automated Enforcement and the Rule of Law,’ *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12, no. 1 (2021): 1–14, at 6–8.

²⁸Regulation (EU) 2024/1689, arts. 6–7 and Annex III; on the staggered timeline, see arts. 111–113.

²⁹Regulation (EU) 2024/1689, Annex III, paras. 6–8.

The Product Liability Directive, recast in 2024 as Directive (EU) 2024/2853 with effect from 9 December 2024 and a national transposition deadline of 9 December 2026, for the first time brings software, including AI systems, within the definition of a “product” capable of giving rise to strict liability for damage caused by a defect.³⁰ This extension is significant for AI-based GI traceability tools because it means that a developer or, in some circumstances, an economic operator that substantially modifies such a tool could in principle be strictly liable where a defect in the system, for example a systematically biased fraud-detection algorithm, causes recoverable damage. The Directive's expanded definition of recoverable damage, which now includes the destruction or corruption of data and medically recognised psychological harm, further broadens the potential scope of exposure.³¹ Yet the Directive, like the AI Act, was not drafted with intellectual property enforcement errors specifically in mind, and it leaves unresolved the more particular question, addressed in Part V, of how liability should be allocated where an AI system wrongly flags a legitimately produced GI product as counterfeit, or conversely fails to detect a genuine instance of infringement.

V. Regulatory Gaps at the Intersection of GI Enforcement and AI Governance

Drawing together the analysis of Parts II to IV, this Part identifies five distinct regulatory gaps that together constrain the legally secure deployment of AI-based traceability for GI enforcement.

1. The absence of technology-specific enforcement standards within the GI regime itself.

Regulation (EU) 2024/1143 mandates risk-based official controls and permits producer-group monitoring but is technologically neutral: it neither requires nor specifically authorises the use of AI-based verification tools, nor does it set any minimum accuracy, auditability, or explainability standard for such tools where they are in fact used.³² The implementing rules adopted alongside the Regulation, including Commission Implementing Regulation (EU) 2025/26 on registration, enforcement, and communication procedures, likewise do not address AI-based verification, leaving producer groups and national authorities to develop practice without a common technical or evidentiary baseline.³³ This silence creates evidentiary uncertainty: it is unclear what weight a national court or administrative authority

³⁰Directive (EU) 2024/2853, art. 4(1) (definition of product), art. 2 (temporal scope); see also Hogan Lovells, EU Introduces Comprehensive Digital-Era Product Liability Directive, Client Note (London, 2024).

³¹Directive (EU) 2024/2853, art. 6.

³²Regulation (EU) 2024/1143, art. 41.

³³Commission Implementing Regulation (EU) 2025/26 of 30 October 2024 Laying Down Rules for the Application of Regulation (EU) 2024/1143 as Regards Registrations, Amendments, Cancellations, Enforcement of Protection, Labelling and Communication, OJ L, 18 January 2025.

should give to an AI-generated fraud flag in the absence of any statutory standard against which its reliability can be assessed.

2. Ambiguous risk classification of producer-group-operated enforcement AI under the AI Act.

As discussed in Part IV, the AI Act's high-risk category for law-enforcement-adjacent AI is framed principally around deployment by a “public authority or on behalf of a public authority.”³⁴ GI enforcement, uniquely among EU intellectual property regimes, is structured around a hybrid public-private model in which recognised producer groups perform a genuine, statutorily recognised monitoring function that is neither wholly private commercial activity nor formal public-authority action. The AI Act does not squarely address this intermediate category, leaving open whether a blockchain-based fraud-detection tool operated by a producer group should be treated as high-risk, as limited-risk subject only to transparency duties under Article 50, or as falling outside Annex III altogether. The practical consequence is that materially similar tools may be subject to substantially different compliance obligations depending solely on whether the operating entity is characterised as public or private, a distinction that maps poorly onto the collaborative structure of GI enforcement.

3. Unresolved data-protection questions arising from supply-chain surveillance.

Traceability systems that identify individual producers, cooperative members, or hauliers engage the GDPR, yet neither Regulation (EU) 2024/1143 nor its implementing rules provide a GI-specific legal basis for this processing, leaving controllers to rely on the general legitimate-interests basis under Article 6(1)(f) GDPR, a basis that requires a case-by-case balancing exercise and offers correspondingly less legal certainty than a specific statutory basis would.³⁵ The position is complicated further by the automated-decision-making safeguards in Article 22 GDPR discussed in Part IV: where an AI system's flag leads directly to a suspension of certification or a referral for prosecution without meaningful human intervention, the producer affected may have a right to obtain human review and to contest the decision, yet the GI Regulation does not specify a corresponding procedural pathway, creating a risk that GDPR-compliant automated enforcement and GI-compliant official controls develop along parallel, uncoordinated procedural tracks.

4. An unallocated liability gap for algorithmic misidentification.

The new Product Liability Directive extends strict liability to defective AI systems and broadens recoverable damage, but its central concept of “defect” is calibrated to safety

³⁴Regulation (EU) 2024/1689, Annex III, para. 6.

³⁵Regulation (EU) 2016/679, art. 6(1)(f); Mireille van Eechoud (n. 20), 9–10.

expectations, asking whether a product does not provide the safety that a person is entitled to expect, rather than to the accuracy of an intellectual-property enforcement determination.³⁶ It is doubtful whether a fraud-detection model's mistaken flag of a legitimate GI product as counterfeit, causing reputational and commercial harm to the affected producer, would readily be characterised as a “defect” in this safety-oriented sense, as distinct from an ordinary administrative or contractual error attributable to the operating producer group or public authority rather than to the technology developer. Conversely, a system's failure to detect genuine infringement causes harm primarily to the GI's collective reputation and to consumers, neither of whom is an obvious claimant under a product-liability framework oriented toward the safety of individual users. The result is a liability gap: harm caused by algorithmic misidentification in the GI enforcement context does not map cleanly onto either the Product Liability Directive's safety-based defect standard or any GI-specific liability rule, because none currently exists.

5. Fragmented competent-authority arrangements for online enforcement under the Digital Services Act.

Article 43 of Regulation (EU) 2024/1143 classifies online GI infringement as illegal content and permits orders to act under Article 9 of the Digital Services Act, but, as noted in Part II, it leaves the designation of the competent national authority entirely to Member States, without prescribing a minimum technical capacity or requiring the use of any particular verification methodology.³⁷ Because AI-based monitoring tools are most naturally suited to generating the volume of online leads that would justify systematic use of the Digital Services Act order mechanism, the absence of a harmonised competent-authority framework risks producing significant disparities between Member States in the practical effectiveness of online GI enforcement, undermining the Regulation's own stated objective of strengthening protection in digital marketplaces.

These five gaps are cumulative rather than independent, and the interaction between them is often more significant than any single gap taken in isolation. A producer group facing an unclear AI Act classification, for example, is simultaneously uncertain of its GDPR processing basis for the underlying traceability data, since the applicable AI Act tier informs the risk assessment that Article 35 GDPR requires before high-risk processing may lawfully begin. Equally, the absence of a designated competent authority for Digital Services Act orders under Article 43 of Regulation (EU) 2024/1143 compounds the liability gap identified above, because it is often unclear which body, if any, bears responsibility for verifying an AI-generated online

³⁶Directive (EU) 2024/2853, art. 7 (defectiveness).

³⁷Regulation (EU) 2024/1143, art. 43; Regulation (EU) 2022/2065, art. 9.

infringement flag before it results in platform-level removal action, leaving affected sellers without a clear addressee for any challenge.

VI. Stakeholder Impacts: Producers, Consumers, and Supply-Chain Actors

The regulatory gaps identified in Part V do not fall evenly across the range of actors affected by GI enforcement. For producer groups, particularly the smaller, often cooperative-structured groups that register the majority of protected GIs, the absence of technology-specific standards and the ambiguous AI Act classification of producer-group-operated tools combine to create both a compliance and a competitiveness problem: without clear guidance, a producer group cannot easily determine what level of AI Act compliance, if any, its traceability investment requires, while the fixed costs of deploying such systems are more easily absorbed by producer groups for high-value GIs than by smaller groups, risking a two-tier enforcement landscape in which well-resourced GIs benefit from proactive AI monitoring while others remain dependent on under-resourced official controls.³⁸

For consumers, AI-based traceability offers a genuine prospect of stronger authenticity assurance, addressing the information asymmetry that GI protection is fundamentally designed to correct.³⁹ That benefit is accompanied, however, by the largely invisible data-protection costs discussed in Part V: consumer-facing traceability applications that allow scanning of a product to verify its GI status frequently draw on the same underlying supply-chain data that identifies individual producers, and consumers are typically not in a position to assess how that data is processed, retained, or reused, an asymmetry the GDPR's transparency obligations only partially address.

Supply-chain intermediaries, including hauliers, packers, and distributors, occupy a particularly exposed position under the current framework. They are frequently the individuals or small businesses whose data populates traceability systems, placing them within the scope of GDPR processing without any bespoke procedural protection, while the unallocated liability gap identified in Part V means that an intermediary wrongly implicated by an AI flag, for instance where a shipment is mistakenly associated with an infringing consignment, has no clearly designated route to challenge or seek redress for that determination, whether through the GI Regulation, the GDPR, or the Product Liability Directive.

The distributional picture is further complicated by the fact that GI producer groups vary enormously in scale, from single-estate wine appellations with sophisticated commercial infrastructure to smallholder cooperatives producing regional cheeses, cured meats, or handicrafts under Regulation (EU) 2023/2411. A regulatory

³⁸On the resource disparities among GI producer groups generally, see European Commission (n. 5), 22–26.

³⁹Michael Blakeney (n. 4), 258–260.

framework calibrated only to the high end of this spectrum risks entrenching, rather than correcting, the enforcement disparities that the 2024 reform of the GI regime was intended to reduce.⁴⁰

VII. Towards Reform: Recommendations

Addressing the gaps identified in Part V does not, in the article's assessment, require wholesale legislative reform of either the GI regime or the AI governance framework; the more proportionate and administratively realistic path lies through targeted implementing measures and interpretive clarification within the structures that already exist.

First, the Commission should use its implementing powers under Regulation (EU) 2024/1143, most naturally through an amendment or supplement to Implementing Regulation (EU) 2025/26, to establish minimum technical standards for AI-based verification tools used in official controls or producer-group monitoring, covering data provenance, auditability, and a floor for human review before an AI-generated flag results in adverse action against a producer.⁴¹ Second, the Commission or the European AI Office should issue interpretive guidance clarifying how the AI Act's high-risk criteria apply to AI systems operated by recognised producer groups performing statutorily recognised monitoring functions under Article 41 of Regulation (EU) 2024/1143, so that the applicable compliance tier turns on the function performed and the consequences for affected producers, rather than on the incidental public or private status of the operating body.

Third, a GI-specific processing basis, or at minimum sector guidance from the European Data Protection Board, should clarify the lawful basis and applicable safeguards for supply-chain traceability data, together with a defined human-review pathway that satisfies Article 22 GDPR where an automated flag leads to certification suspension or referral for prosecution. Fourth, the interaction between the Product Liability Directive and GI-specific harms should be clarified, whether through Commission guidance on the interpretation of "defect" in the context of enforcement-oriented AI, or through a bespoke allocation-of-liability provision within the GI Regulation's own implementing framework, so that neither producers wrongly flagged nor consumers exposed to undetected counterfeits are left without a clearly identifiable route to redress.

Fifth, Member States should be required, through amendment of Article 43 of Regulation (EU) 2024/1143 or through coordinated Commission guidance, to designate a specific competent authority for Digital Services Act orders relating to GI infringement, mirroring the model already adopted for cross-border coordination in

⁴⁰On the diversity of GI producer-group structures across Member States, see European Commission (n. 5), 8–12.

⁴¹Cf. Regulation (EU) 2024/1143, art. 41(5), which already empowers the Commission to adopt delegated acts specifying further control requirements.

the air-quality context under the Commission for Air Quality Management, which demonstrates that a dedicated, adequately resourced coordinating body can meaningfully improve the practical effectiveness of a Union-wide standard applied through decentralised national action.⁴² Finally, targeted EU funding, whether through the common agricultural policy's producer-group support measures or a dedicated digital-traceability facility, should be directed toward smaller producer groups to prevent the emergence of a two-tier enforcement landscape identified in Part VI.

VIII. Conclusion

The European Union's geographical indications regime, substantially reformed in 2024, provides a comparatively sophisticated framework for the registration and, in principle, the enforcement of GI rights, and it has for the first time extended explicit protection into the online environment. Artificial intelligence-based traceability technologies offer a genuinely promising means of closing the long-standing gap between the scale of the GI enforcement task and the administrative capacity available to address it, converting a reactive, complaint-driven model into a more proactive and preventive one. Yet the EU's parallel regulatory architecture governing AI, comprising the GDPR, the AI Act, and the recast Product Liability Directive, was not designed with GI enforcement in view, and this article has identified five specific points at which the two regimes fail to interlock: the absence of technology-specific enforcement standards within the GI Regulation itself; the ambiguous AI Act classification of producer-group-operated enforcement tools; unresolved data-protection questions arising from supply-chain surveillance; an unallocated liability gap for algorithmic misidentification; and fragmented competent-authority arrangements for online enforcement under the Digital Services Act. None of these gaps is intractable, and each admits of a targeted, implementing-level solution of the kind proposed in Part VII. What the analysis suggests, more fundamentally, is that as AI-based tools migrate from purely commercial into regulatory and enforcement contexts, sector-specific legislation such as the GI Regulation can no longer be drafted, or subsequently amended, without express attention to its interaction with the Union's horizontal AI governance framework, if the promise of proactive, technology-enabled enforcement is to be realised without displacing legal certainty for the producers, consumers, and intermediaries the GI regime exists to protect.

⁴²On the Commission for Air Quality Management as an example of institutionalised cross-jurisdictional coordination, see PRS Legislative Research, *The Commission for Air Quality Management in National Capital Region and Adjoining Areas Bill, 2021*, Bill Summary (New Delhi, 2021).

Bibliography

- Abbott, Ryan. *The Reasonable Robot: Artificial Intelligence and the Law*. Cambridge: Cambridge University Press, 2020.
- Agrinfo. *Revision of the EU Geographical Indications Scheme*. EU Agri-Food Trade Policy Briefing, 2024.
- Blakeney, Michael. 'Geographical Indications and International Trade.' *Journal of World Intellectual Property* 17, no. 6 (2014): 252–265.
- Bonadio, Enrico. 'Protection of Geographical Indications in the European Union: An Overview.' *International Review of Intellectual Property and Competition Law* 50 (2019): 547–568.
- Bonadio, Enrico, and Alexandra George. 'Artificial Intelligence as a Tool for Trade Mark and Geographical Indication Enforcement.' *European Intellectual Property Review* 42, no. 8 (2020): 473–480.
- Calboli, Irene, and Edward Lee, eds. *Research Handbook on Intellectual Property and Geographical Indications*. Cheltenham: Edward Elgar, 2016.
- De Filippi, Primavera, and Aaron Wright. *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press, 2018.
- European Commission. *Evaluation of the EU Geographical Indications System*. Commission Staff Working Document, SWD(2021) 264 final. Brussels, 2021.
- European Parliament, European Parliamentary Research Service. *Artificial Intelligence and Intellectual Property Rights*. EPRS Study. Brussels, 2020.
- European Union Intellectual Property Office. *Intellectual Property Infringements and Enforcement in the Digital Environment*. EUIPO Observatory Report. Alicante: EUIPO, 2020.
- Gangjee, Dev. *Relocating the Law of Geographical Indications*. Cambridge: Cambridge University Press, 2012.
- Malgieri, Gianclaudio. 'Data Protection and Artificial Intelligence in Europe.' *European Data Protection Law Review* 5, no. 1 (2019): 3–12.
- Organisation for Economic Co-operation and Development. *Enhancing the Use of Traceability Technologies in Global Supply Chains*. Paris: OECD Publishing, 2019.
- PRS Legislative Research. *The Commission for Air Quality Management in National Capital Region and Adjoining Areas Bill, 2021*. Bill Summary. New Delhi, 2021.
- Van Eechoud, Mireille. 'Automated Enforcement and the Rule of Law.' *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 12, no. 1 (2021): 1–14.
- World Intellectual Property Organization. *World Intellectual Property Report 2022: The Direction of Innovation*. Geneva: WIPO, 2022.

Table of EU Legislation

Treaty on the Functioning of the European Union, OJ C 326, 26 October 2012.

Council Directive 85/374/EEC of 25 July 1985 on Liability for Defective Products, OJ L 210, 7 August 1985 (repealed).

Regulation (EU) No 1151/2012 of the European Parliament and of the Council of 21 November 2012 on Quality Schemes for Agricultural Products and Foodstuffs, OJ L 343, 14 December 2012 (repealed).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4 May 2016.

Regulation (EU) 2017/625 of the European Parliament and of the Council of 15 March 2017 on Official Controls, OJ L 95, 7 April 2017.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act), OJ L 277, 27 October 2022.

Regulation (EU) 2023/2411 of the European Parliament and of the Council of 18 October 2023 on the Protection of Geographical Indications for Craft and Industrial Products, OJ L, 16 November 2023.

Regulation (EU) 2024/1143 of the European Parliament and of the Council of 11 April 2024 on Geographical Indications for Wine, Spirit Drinks and Agricultural Products, OJ L, 23 April 2024.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), OJ L, 12 July 2024.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products, OJ L, 18 November 2024.

Commission Implementing Regulation (EU) 2025/26 of 30 October 2024, OJ L, 18 January 2025.