Cambridge Law Review (2025) Vol 10, Issue 2, 77–100

Algorithmic Tacit Collusion: Addressing the Gaps in Article 101(1)(a) of the TFEU

EMMA MINERVA BRAMBILLA*

ABSTRACT

This article explores the emergent risk of algorithmic tacit collusion via supra-competitive price fixing and the challenges it poses to European Union ('EU') competition law under article 101(1)(a) of the Treaty on the Functioning of the European Union ('TFEU'). With the proliferation of self-learning dynamic pricing algorithms operating on deep learning models, undertakings may unwittingly enable autonomous systems to coordinate prices without human input or explicit agreements. This 'Digital Eye' scenario—where algorithms independently identify collusion as a profit-maximising strategy—highlights a growing enforcement gap. The article critically examines whether such behaviour could fall within the definitions of 'concerted practice' and 'by object' restriction under existing legal doctrine, arguing for a purposive reinterpretation of article 101(1)(a) of the TFEU in the light of technological change. Furthermore, it assesses the legal accountability of both developers and users of collusive algorithms, proposing liability frameworks, including strict product liability, joint liability, and vicarious liability. Finally, it advocates for ex ante regulatory measures—such as algorithmic design constraints, mandatory audits, and compliance certifications—to future-proof competition law. The article contends that, unless proactive legal adaptation occurs, firms may exploit regulatory ambiguity to the detriment of fair market competition and consumer welfare in the Digital Internal Market.

Keywords: algorithms, competition law, price fixing, tacit collusion

I. INTRODUCTION

Artificial Intelligence ('AI')—a branch of science that develops computer programs aimed at performing tasks requiring human-like intelligence—has emerged as a transformative force, revolutionising market dynamics and competition enforcement mechanisms.[1] Algorithms—structured sequences of computational steps designed to transform input data into desired outputs—constitute the essence of AI.[2] Owing to their multifaceted manifestations, they wield significant influence in shaping the contemporary landscape of competition within the EU. A

* LLM, London School of Economics and Political Science (2025); LLB, University of Groningen (2024).

[1] Fathima Anjila PK, 'Artificial Intelligence', in J Karthikeyan, Ting Su Hie and Ng Yu Jin (eds), *Learning Outcomes of Classroom Research* (L'Ordine Nuovo Publication 2021) 65.

[2] Thomas H Cormen and others, *Introduction to Algorithms* (4th edn, MIT Press 2022) 5.

category of algorithms that is widely utilised by undertakings is pricing algorithms.[3] Historically, *static* pricing algorithms,[4] limited to a finite number of responses to specific situations and subject to change only following the coders' intervention, have long aided industries where demand fluctuates quicker than supply, such as the transport and hospitality industries.[5] Nowadays, any industry takes advantage of pricing algorithms (specifically, *dynamic* pricing algorithms).[6] These algorithms are designed to optimise an undertaking's market performance by dynamically (that is, *continuously* and *automatically*) adjusting prices based on various real-time factors such as demand, competitor pricing, and market conditions.[7] Their purpose is to enhance profitability and competitiveness while adapting to fluctuations in the market landscape.[8] As a result, they have become ubiquitous tools within the market (both offline and online), where small, medium, and large-sized undertakings leverage them to optimise their performance (through, for instance, profit maximisation).[9]

However, the way of achieving this objective may raise concerns about potential anti-competitive behaviour. This holds especially true for dynamic pricing algorithms operating on an unsupervised-learning paradigm, often dubbed 'autonomous' or 'self-learning' because of their ability *autonomously* to learn the optimal (that is, instantaneous and extremely accurate) method to achieve the objective for which they are initially programmed.[10] In fact, unlike static algorithms, self-learning dynamic algorithms can autonomously, automatically, and continuously adjust to changes in their environment—particularly those functioning on a deep learning ('DL') model, which use multi-layered artificial neural networks that mimic human neurons and iteratively learn from the data they encounter.[11] As such, these algorithms decide *how* to perform tasks in unknown and evolving settings with no human instruction, after the initial programmed objective.[12]

Accordingly, they constitute a valuable tool for undertakings seeking to improve their market performance in a fast-changing environment,[13] such as the EU Digital Internal Market. Nevertheless, these algorithms may autonomously learn that *collusion* via price fixing at a

[3] For clarity, 'pricing algorithms' in this article refer solely to algorithms that establish an output price. Other algorithms related to prices but performing different tasks, such as price tracking or price personalisation, are not included.

[4] These algorithms are also referred to as 'heuristic' or 'expert': see for example Michal S Gal, 'Algorithms as Illegal Agreements' (2019) 34 Berkeley Technology Law Journal 68, 78; Oxera, 'When Algorithms Set Prices: Winners and Losers' (19 June 2017) 5 <https://www.regulation.org.uk/library/2017-Oxera-When_algorithms_set_prices-winners_and_losers.pdf> accessed 7 May 2024.

[5] Philip Hanspach and Niccolò Galli, 'Collusion by Pricing Algorithms in Competition Law and Economics' (2024) EUI RSC Working Paper 2024/06, 7–9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4732527> accessed 13 April 2024.

[6] ibid.

[7] Valeria Caforio, 'Algorithmic Tacit Collusion: A Regulatory Approach' (2023) 15 Competition Law Review 9, 11–14.

[8] ibid.

[9] ibid.

[10] ibid.

[11] See OECD, 'Algorithmic Competition: OECD Competition Policy Roundtable Background Note' (OECD, 2023) 9 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/05/algorithmic-competition_2be02d00/cb3b2075-en.pdf> accessed 12 April 2024. See also Rahil Mammadov, 'The Rising Role of Pricing Algorithms: Positive and Negative Effects in the Framework of EU Competition Law' (Master's thesis, Lund University 2022) 9 <https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9080831&fileOId=9086028> accessed 12 April 2024.

[12] See for example Caforio (n 7); Hanspach and Galli (n 5) 7–8.

[13] Hanspach and Galli (n 5) 7–8.

supra-competitive level is the optimal means to achieve the profit maximisation goal.[14] Such a phenomenon can be labelled as algorithmic *tacit* collusion via price fixing (also referred to as 'machine-to-machine cooperation' or 'algorithmic interdependent pricing'[15]). In fact, contrary to algorithmic *explicit* collusion, where algorithms are employed as facilitators, strengtheners, and enablers of human collusion, algorithmic tacit collusion occurs without any human involvement or reciprocal interaction.[16] Notably, the legal standard for collusion via price fixing, corresponding to the formation of a 'cartel',[17] entails any coordination between competing undertakings—achieved via an 'agreement' or 'concerted practice'—to raise,[18] lower, or stabilise prices, or competitive terms.[19] Pursuant to article 101(1)(a) of the TFEU,[20] such conduct is expressly prohibited, as it is considered inherently detrimental to competition and devoid of any outweighing efficiencies.[21] Within the EU Digital Internal Market, pricing algorithms are extensively utilised. For instance, in a 2017 inquiry by the EU Commission into the e-commerce sector, 53 per cent of respondent retailers reported tracking online prices of competitors.[22] Among these, 67 per cent stated their use of automatic software programs for this purpose and as part of their operational strategies.[23] Furthermore, remarkably, the Court of Justice of the European Union ('CJEU') has already acknowledged and addressed the concern of anti-competitive behaviour facilitated *through* the use of pricing algorithms in the *AC-Treuhand AG v Commission*[24] and *'Eturas' UAB v Lietuvos Respublikos konkurencijos taryba ('Eturas')*[25] rulings.

However, at present, there are no documented cases of algorithmic tacit collusion, where self-learning dynamic pricing algorithms, operating on a DL model, engage *by themselves* in collusion via supra-competitive price fixing. Nevertheless, numerous scholars and policymakers suggest that such instances may occur in the future. From an enforcement perspective, this new theory of harm (that is, a framework to conceptualise and describe the

[14] See for example ibid 17; Sophie Devogele, 'Algorithmic Tacit Collusion: A Threat to the Current EU Competition Law Framework?' (LLM thesis, Tilburg University 2023) 2–3 <https://mededingingscongres.nl/wp-content/uploads/2023/10/Thesis-final-version-PDF.pdf> accessed 23 April 2024. For clarity, in the light of the evidence and academic sources currently available, this article focuses solely on horizontal price fixing (that is, between competing undertakings) at supra-competitive levels. However, the possibility of vertical anti-competitive conduct by self-learning algorithms or low-level price fixing achieving other programmed objectives, should not be dismissed outright.

[15] Caforio (n 7) 10.

[16] ibid.

[17] Alison Jones, Brenda Sufrin and Niamh Dunne, Jones & Sufrin's *EU Competition Law: Text, Cases, and Materials* (8th edn, OUP 2023) 670–71; OECD, 'Recommendation of the Council Concerning Effective Action against Hard Core Cartels' (25 March 1998) 3 <https://one.oecd.org/document/C(98)35/FINAL/en/pdf> accessed 20 May 2024.

[18] Empirical studies indicate that cartel pricing typically exceeds competitive levels by more than 10 per cent and sometimes in excess of 20 per cent: see Jones, Sufrin and Dunne (n 17) 660.

[19] See for example Ioannis Kokkoris and Claudia Lemus, 'Price-Fixing Agreement' (*Concurrences*) <https://www.concurrences.com/en/dictionary/price-fixing-agreement> accessed 5 May 2024; Jones, Sufrin and Dunne (n 17) 671–74.

[20] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/1 ('TFEU').

[21] Jones, Sufrin and Dunne (n 17).

[22] European Commission, 'Commission Staff Working Document Accompanying the Document: Report from the Commission to the Council and the European Parliament, Final Report on the E-commerce Sector Inquiry', SWD (2017) 154 final, para 149; Jones, Sufrin and Dunne (n 17) 687; Tobias Werner, 'Algorithmic and Human Collusion' (2023) DICE Discussion Paper No 372, 1 <https://www.econstor.eu/bitstream/10419/246229/1/1777327733.pdf> accessed 13 April 2023.

[23] European Commission, 'Commission Staff Working Document' (n 22).

[24] Case C-194/14 P *AC-Treuhand AG v Commission*, EU:C:2015:717.

[25] Case C-74/14 *'Eturas' UAB v Lietuvos Respublikos konkurencijos taryba*, EU:C:2016:42.

harm stemming from specific types of conduct in a market[26]), coined as the 'Digital Eye' by Ariel Ezrachi and Maurice Stucke, presents notable tiers of *legal uncertainty* under EU competition law.[27]

Indeed, first of all, algorithmic tacit collusion represents a resurgence of the 'oligopoly problem', wherein tacit collusion evades formal condemnation under article 101(1) of the TFEU, which exclusively addresses explicit collusion.[28] This exemption is due to (i) the risk of erroneously penalising an actual parallel conduct and (ii) the infrequency of such scenarios in practical application.[29] Thus, if algorithmic tacit collusion materialises, it is uncertain whether it would fall within the scope of article 101(1). Secondly, there is ambiguity surrounding whether algorithmic tacit collusion via supra-competitive price fixing would be categorised as an 'agreement' or as a 'concerted practice' under article 101(1) of the TFEU. Thirdly, another question arises as to whether such conduct would be classified as a restriction 'by object' under article 101(1)(a). Fourthly, uncertainty remains about who should be held accountable and how liability should be determined for potential violations of competition law.

If, or when, algorithmic tacit collusion via supra-competitive price fixing materialises, the challenges to legal certainty that have been outlined above will significantly impede the enforcement of article 101(1)(a) of the TFEU, potentially creating an exploitable legal loophole for competing undertakings. Therefore, proactive measures must be taken ex ante to address these uncertainties and safeguard competition. In the light of this background, this article seeks to answer the following questions: first, could article 101(1)(a) of the TFEU catch algorithmic tacit collusion via supra-competitive price fixing and, if so, how? And, secondly, what ex ante measures could be implemented to address the legal uncertainty arising from the materialisation of the 'Digital Eye'?

II. ALGORITHMIC (TACIT) COLLUSION: A NARRATIVE

This section examines how pricing algorithms have evolved and how they are increasingly implicated in anti-competitive conduct, which sets the stage for understanding the emerging risk of algorithmic tacit collusion in EU competition law under article 101(1)(a) of the TFEU.

A. PRICING ALGORITHMS: EVOLUTION AND FUNCTIONING

Since the inception of computer science technology in the 1940s, algorithms have been integral in performing diverse computational tasks, encompassing mathematical calculations, as well as sorting and searching operations. Importantly, the advent of the Internet in the 1990s, and the proliferation of AI, marked a pivotal juncture in the evolution of algorithms: the proliferation of digital markets catalysed the development of pricing algorithms, which utilise prices as inputs and employ computational methodologies to determine optimal pricing outputs to, for instance, maximise a firm's profit.[30]

[26] Marios C Iacovides, *The Law and Economics of WTO Law: A Comparison with EU Competition Law's 'More Economic Approach'* (Edward Elgar Publishing 2021) 122–41.
[27] Ariel Ezrachi and Maurice E Stucke, 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' (2017) 2017 University of Illinois Law Review 1775, 1795.
[28] Jones, Sufrin and Dunne (n 17) 669.
[29] Caforio (n 7) 12.
[30] Mammadov (n 11) 14–15.

The most transformative step has been the emergence of *self-learning dynamic pricing algorithms*, operating on DL models. These systems process vast, multidimensional datasets through artificial neural networks that mimic human neurons, enabling them to select, process, and predict outcomes at a speed and precision beyond human capacity.[31] Input data may derive from both internal firm information (production costs, inventories, orders) and external real-time factors (competitors' prices, demand fluctuations, consumer behaviour).[32] Crucially, once programmed with the single objective of profit maximisation, these algorithms continuously adjust their outputs in real time without further human intervention.[33] Their unilateral and autonomous nature raises acute concerns under EU competition law. By replacing human decision-makers, DL pricing algorithms may independently discover that supra-competitive price fixing is the most effective strategy to achieve their objective.[34] Scholars warn that such collusion can arise significantly faster than human coordination, narrowing the scope for detection or intervention.[35] The risks are exacerbated by the 'black box' opacity of DL: programmers cannot retrace or predict the decision-making process, making it impossible to know whether a supra-competitive outcome results from lawful parallel conduct or from algorithmic tacit collusion.[36]

B. ANTI-COMPETITIVE USE OF PRICING ALGORITHMS

The increasing reliance on pricing algorithms has prompted concern that such tools may facilitate collusion in novel ways. The literature identifies four principal theories of harm: the 'Messenger', the 'Hub and Spoke', the 'Predictable Agent', and the 'Digital Eye'.[37] While the first three theories already find support in enforcement practice, the 'Digital Eye' remains hypothetical, underscoring an unresolved gap in the scope of article 101(1)(a) of the TFEU.

The 'Messenger' theory describes a situation where algorithms are deployed to stabilise or reinforce an existing cartel agreement. In these cases, the software is deliberately programmed to monitor rivals and adjust prices in line with collusive strategies.[38] A leading example is the *Online Sales of Posters and Frames* decision of the UK's Competition and Markets Authority, in which two online poster sellers used pricing algorithms to maintain pre-agreed prices on the Amazon marketplace, thereby avoiding undercutting each other.[39] Similarly, in 2020 the Spanish National Commission for Markets and Competition opened proceedings against several real estate platforms on the basis that algorithms embedded in

[31] See for example ibid; OECD, 'Algorithmic Competition' (n 11) 6–9.

[32] Autorité de la Concurrence and Bundeskartellamt, 'Algorithms and Competition' (November 2019) 9 <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf?__blob=publicationFile&v=3> accessed 28 April 2024.

[33] In fact, these algorithms are also referred to as 'repricing' algorithms: see Hanspach and Galli (n 5).

[34] See for example Caforio (n 7) 9–13; ibid 7–9; Devogele (n 14).

[35] Matthias Hettich, 'Algorithmic Collusion: Insights from Deep Learning' (24 November 2021) 1 <http://dx.doi.org/10.2139/ssrn.3785966> accessed 25 May 2024.

[36] Caforio (n 7) 14.

[37] Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016) 35–71.

[38] ibid.

[39] CMA Infringement Decision, *Online Sales of Posters and Frames* (Case 50223, 12 August 2016) paras 1.3, 3.46, 3.62–3.93 <https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf> accessed 25 May 2024.

brokerage software aligned agents' pricing and sales terms.[40] Both instances illustrate that algorithms can serve as the operational tool for explicit collusion. The legal significance of such cases lies in confirming that algorithmic implementation of cartels does not alter their legal character: they remain agreements or concerted practices prohibited by article 101 of the TFEU.

The 'Hub and Spoke' theory arises where a central platform or intermediary employs algorithms to coordinate the behaviour of otherwise competing undertakings.[41] The jurisprudence of the CJEU already provides a doctrinal basis for facilitator liability. In *AC-Treuhand*, the court held that a consultancy that actively contributed to the organisation of cartel meetings and the monitoring of collusive arrangements could itself be liable under article 101 of the TFEU.[42] Although not directly concerning algorithms, the reasoning has clear implications for digital platforms. National authorities have extended this principle: the Danish Competition and Consumer Authority found that the platform, Ageras, infringed national competition law by supplying 'estimated market prices' and 'minimum quotes' to service providers,[43] while the Romanian Competition Council expressed concern in 2020 that ride-hailing platforms' pricing algorithms could facilitate collusion.[44] These cases illustrate that the role of digital intermediaries in orchestrating anti-competitive outcomes is not peripheral, but central, and that liability may attach where their algorithmic tools function as a coordinating hub.

Under the 'Predictable Agent' theory, collusion is enabled not by direct communication but by the transparency and predictability that algorithms create. By encoding pricing strategies or revealing rivals' intentions, algorithms reduce market uncertainty and facilitate convergence.[45] The *Eturas* ruling is the paradigmatic instance of this.[46] Here, an online booking platform imposed a uniform cap on discounts through its internal messaging system and technical restrictions in its software. The CJEU held that travel agencies could be presumed to have been aware of the restriction and were therefore liable under article 101 of the TFEU.[47] More recently, in 2022, the Italian Competition Authority investigated abnormal convergence of airline ticket prices on routes to Sicily, noting that algorithms may have facilitated supra-competitive pricing.[48] These examples underscore that, even where explicit agreement is absent, the technical design of algorithms may create functional equivalence to collusion by stabilising expectations and reducing incentives to compete.

[40] National Commission for Markets and Competition, 'The CNMC Opens Antitrust Proceedings against Seven Firms for Suspected Price Coordination in the Real Estate Intermediation Market' (19 February 2020) <https://www.cnmc.es/sites/default/files/editor_contenidos/Notas de prensa/2020/2020219 NP Intermediation Market EN.pdf> accessed 14 April 2024.

[41] Ezrachi and Stucke, 'Artificial Intelligence' (n 27).

[42] *AC-Treuhand* (n 24) paras 36–39.

[43] 'Danish Competition Council: Ageras Has Infringed Competition Law' (*Danish Competition and Consumer Authority*, 30 June 2020) <https://en.kfst.dk/nyheder/kfst/english/decisions/20200630-danish-competition-council-ageras-has-infringed-competition-law> accessed 25 May 2024.

[44] See Sheng Li, Claire Chunying Xie and Emilie Feyler, 'Algorithms & Antitrust: An Overview of EU and National Case Law' (Concurrences, 7 October 2021) <https://www.concurrences.com/en/bulletin/special-issues/algorithms-competition/algorithms-antitrust-an-overview-of-eu-and-national-case-law> accessed 25 May 2024.

[45] *AC-Treuhand* (n 24) paras 36–39.

[46] *Eturas* (n 25) paras 19–21.

[47] ibid.

[48] Provvedimento n 30408, *Prezzo Biglietti Aerei da e per la Sicilia nel Periodo Natalizio* (Case I863, 20 December 2022)<https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/EA131DE0E183BC70C1258925004D308C/$File/p30408.pdf> accessed 25 May 2024.

The final theory of harm, the 'Digital Eye', is qualitatively distinct. It envisages a scenario of algorithmic tacit collusion in which undertakings independently deploy self-learning, dynamic pricing algorithms that, when exposed to similar data sets and optimisation objectives, autonomously converge on supra-competitive outcomes.[49] Unlike the first three theories, no human communication or intentional coordination is required: collusion arises from the interaction of algorithms themselves. To date, no EU or national authority has sanctioned conduct under this model. The absence of precedent is itself significant. Whereas 'Messenger', 'Hub and Spoke', and 'Predictable Agent' scenarios can be accommodated within the existing framework of article 101 of the TFEU as explicit collusion, the 'Digital Eye' resists classification because it lacks the element of agreement or concerted practice that is traditionally required. This gap points to a pressing enforcement challenge: if algorithmic tacit collusion materialises in practice, the current legal framework may be inadequate to address it.

III. Algorithmic Tacit Collusion via Price Fixing under Article 101(1)(A) of the TFEU

This section explores how algorithmic tacit collusion, particularly through supra-competitive price fixing, may be brought within the scope of article 101(1) of the TFEU. It examines, first, whether such practices can be understood as a 'concerted practice' when interpreted in the light of technological developments, and secondly, whether they may be categorised as restrictions *by object* through analogy with traditional price fixing. In doing so, the analysis highlights the risk of an enforcement gap if algorithmic tacit collusion were excluded, especially given its potential to emerge beyond oligopolistic markets and in increasingly digitalised settings.

Within the EU legal framework, the arsenal *par excellence* that prohibits collusion via supra-competitive price fixing is article 101(1)(a) of the TFEU. This article prohibits 'all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market'.[50] Remarkably, the notion of 'undertaking' is broadly interpreted and it encompasses any entity that is engaged in an economic activity, regardless of its legal status and the way it is financed.[51]

On the one hand, an 'agreement' does not necessarily require formalisation to be recognised under article 101(1)(a) of the TFEU. In fact, to encompass a broad spectrum of agreements, the *ACF Chemiefarma NV v Commission* ('*Quinine Cartel*')[52] ruling clarified that informal arrangements are also subject to scrutiny.[53] Furthermore, an agreement is deemed to exist regardless of its formality, whether oral or written, and irrespective of its legal enforceability or absence of provisions for non-compliance.[54] However, in order to fall under the purview of article 101(1) of the TFEU, the agreement requires the concurrence of wills—expressed through the attainment of consensus on a common, defined, and precise plan—

[49] Ezrachi and Stucke, 'Artificial Intelligence' (n 27).
[50] TFEU, art 101(1). In the light of this article's focus on collusion between two or more undertakings, the requirement of 'decisions by associations of undertakings' will not be examined.
[51] Case C-41/90 *Klaus Höfner and Fritz Elser v Macrotron GmbH* [1991] ECR I-1979, para 21.
[52] Case 41-69 *ACF Chemiefarma NV v Commission* [1970] ECR 661.
[53] ibid paras 110–24.
[54] Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* (7th edn, OUP 2020) 1038.

between two or more parties, as distinct from unilateral measures, dictating their conduct within the market in a prescribed manner, whether in action or abstention.[55] The precise form of this concurrence is not important if it constitutes the faithful expression of the parties' intentions.[56] Unilateral measures do not therefore suffice; however, an agreement can be deduced from a party's conduct if the manifestation of the wish of one contracting party to achieve an anti-competitive goal serves as an invitation to the other party, either explicitly or implicitly, to pursue that goal together.[57]

On the other hand, the notion of 'concerted practice' aims to forestall situations where entities collaborate in ways that fall short of an agreement, which may otherwise circumvent the application of article 101(1) of the TFEU.[58] This concept has been elaborated upon in seminal cases such as *Imperial Chemical Industries Ltd v Commission*,[59] which ruled that the purpose of the term was to preclude 'coordination between undertakings which, without having reached the stage where an agreement properly so-called has been concluded, *knowingly* substitutes practical cooperation between them for the risks of competition'.[60] Additionally, *Coöperatieve Vereniging 'Suiker Unie' UA v Commission*[61] clarified that a 'concerted practice' does not necessitate the 'working out of an actual plan' but rather encompasses any 'direct or indirect' contact—a *mental consensus*[62]—between undertakings aimed at influencing the behaviour of competitors or disclosing intended market strategies.[63] It is governed by a presumption that such a practice will be enacted while these undertakings remain active on the market.[64] Consequently, although a 'concerted practice' requires reciprocal cooperation between the parties,[65] it is not necessary to demonstrate a 'meeting of minds' or a 'common course of conduct', nor does the consensus need to be reached verbally.[66] It is enough to demonstrate that, based on a series of indicia, the presence of a 'concerted practice' is the sole plausible explanation for the market outcome.[67]

Although article 101(1) of the TFEU delineates between 'agreements' and 'concerted practices', the CJEU has asserted that this differentiation is merely formal:[68] both address explicit collusion, but, whereas an 'agreement' requires a clearly expressed concurrence of wills, a 'concerted practice' can be established on the basis of less explicit, indirect, or tacit forms of coordination. When applied to algorithmic tacit collusion via price fixing, *three tiers* of legal uncertainty arise, which are discussed below.

[55] ibid 1037–39.
[56] Case C-338/00 P *Volkswagen AG v Commission* [2003] ECR I-9189, paras 63–65.
[57] Joined Cases C-2/01 P and C-3/01 P *Bundesverband der Arzneimittel-Importeure eV v Bayer AG* [2004] ECR I-23, paras 100–02.
[58] Craig and de Búrca (n 54) 1040–43.
[59] Case 48-69 *Imperial Chemical Industries Ltd v Commission* [1972] ECR 619.
[60] ibid para 64 (emphasis added).
[61] Joined Cases 40 to 48, 50, 54 to 56, 111, 113 and 114-73 *Coöperatieve Vereniging 'Suiker Unie' UA v Commission* [1975] ECR 1663 ('*Suiker Unie*').
[62] Richard Whish and David Bailey, *Competition Law* (10th edn, OUP 2021) 118–20.
[63] *Suiker Unie* (n 61) paras 173–74.
[64] See for example Case C-609/13 P *Duravit AG v Commission*, EU:C:2017:46, para 70; Case C-49/92 P *Commission v Anic Partecipazioni SpA* [1999] ECR I-4125, para 115; Case T-344/18 *Rubycon Corp v Commission*, EU:T:2021:637, para 104; Case C-199/92 P *Hüls AG v Commission* [1999] ECR I-4287, para 162.
[65] Jones, Sufrin and Dunne (n 17) 200.
[66] Whish and Bailey (n 62).
[67] See for example ibid; Stefan Thomas, 'Harmful Signals: Cartel Prohibition and Oligopoly Theory in the Age of Machine Learning' (2019) 15 Journal of Competition Law & Economics 159, 180–83.
[68] See for example *Anic Partecipazioni* (n 64) para 131; Case C-8/08 *T-Mobile Netherlands BV v Raad van bestuur van de Nederlandse Mededingingsautoriteit* [2009] ECR I-4529, paras 23–24.

A. ARTICLE 101(1)(A) OF THE TFEU APPLIED TO ALGORITHMIC TACIT COLLUSION VIA PRICE FIXING

In the light of the criteria needed for coordination to be caught by article 101(1) of the TFEU, it is obvious that algorithmic tacit collusion via supra-competitive price fixing—characterised by its *autonomous* and *unilateral* nature as detailed in Section II.A—de facto falls outside the scope of article 101(1)(a) and therefore results in lawful conduct. Consequently, a *first tier* of legal uncertainty arises as to whether such algorithmic tacit collusion via supra-competitive price fixing, if it materialises, will be caught under article 101(1)(a) of the TFEU.

The primary rationale for this de facto exemption of tacit collusion from the purview of article 101(1) lies in the economic theory of 'conscious parallelism'—a rational, natural response in a given market—where undertakings independently adjust their prices in response to the pricing strategies of their competitors, with no element of concertation.[69] This theory finds particular validation within oligopolistic markets—markets with few dominant firms, high entry barriers, and strategic interdependence—as distinct from competitive markets (many firms, no influence) or monopolies (one firm). Their limited differentiation and price transparency make rivals' price changes easily detectable.[70]

However, three arguments—drawing from economic theory, traditional legal principles, and technology-based evidence—can be marshalled to substantiate the contention that algorithmic tacit collusion via supra-competitive price fixing warrants inclusion within the scope of article 101(1)(a) of the TFEU. First, while the conscious parallelism exemption granted to human tacit collusion may be accepted—since there is no 'agreement', parallel conduct may stem from rational independent behaviour, and over-enforcement risks penalising natural oligopoly dynamics—it is seen as an acceptable risk.[71] By contrast, its application to algorithmic tacit collusion is more problematic. Conscious parallelism hinges on market structure, yet digital markets—where self-learning dynamic pricing algorithms are widely deployed—can rapidly shift from competitive to concentrated, thereby enabling oligopolistic outcomes.[72] Moreover, unlike human decision-making, algorithms process vast amounts of data with speed, precision, and constant monitoring, which allows them to detect and replicate rivals' strategies almost instantaneously.[73] As a result, algorithmic tacit collusion not only entrenches coordination more effectively within oligopolies but may also extend beyond them, given the capacity of algorithms to sustain supra-competitive outcomes even in more fragmented markets.[74]

[69] Nicolas Petit, 'The Oligopoly Problem in EU Competition Law' in Ioannis Lianos and Damien Geradin (eds), *Handbook on European Competition Law: Substantive Aspects* (Edward Elgar Publishing 2013) 259–49.
[70] ibid.
[71] Devogele (n 14) 4.
[72] Jonathan S Kanter, 'Digital Markets and "Trends towards Concentration"' (2023) 11 Journal of Antitrust Enforcement 143, 144.
[73] See for example Ai Deng, 'What Do We Know about Algorithmic Tacit Collusion?' (2018) 33 Antitrust 88, 88; OECD, 'Algorithms and Collusion: Competition Policy in the Digital Age' (14 September 2017) 36 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/05/algorithms-and-collusion-competition-policy-in-the-digital-age_02371a73/258dcb14-en.pdf> accessed 13 May 2024; Caforio (n 7) 23.
[74] Caforio (n 7) 10, 23.

Secondly, article 101 of the TFEU was enacted in 1958 as part of the Treaty establishing the European Economic Community,[75] formulated in an era vastly different from today's technological landscape. In this context, employing the traditional legal method of teleological interpretation, which involves interpreting laws in line with their overarching objectives,[76] becomes imperative. Considering the fundamental aim of article 101(1) of the TFEU, which is to safeguard competition in markets to promote current and future consumer welfare and ensure efficient resource allocation,[77] it becomes apparent that the regulatory framework must adapt to contemporary challenges. Thus, in the light of technological advancements and the evolving nature of competition, subjecting algorithmic tacit collusion via supra-competitive price fixing to the ambit of article 101(1)(a) of the TFEU emerges as a compelling necessity. A readiness for such a broader interpretation of EU competition law was already shown by the CJEU in *Meta Platforms Inc v Bundeskartellamt*,[78] where the court accepted that breaches of data protection law—although not traditionally within competition law—could nonetheless fall under article 102 of the TFEU because of their capacity to reinforce dominance and distort competition.[79] By analogy, algorithmic coordination, while not foreseen in the classical framework of article 101, produces supra-competitive outcomes that are functionally equivalent to explicit collusion, thereby warranting an equally adaptive interpretation.

Thirdly, although algorithmic tacit collusion via supra-competitive price fixing remains a theoretical hypothesis, empirical evidence supports its plausibility. Contrary to assertions by some scholars who dismiss it as mere 'fiction' or 'exaggeration',[80] such scepticism warrants rebuttal. The rationale for this rebuttal is straightforward: technological advancements continually reshape our understanding of what is achievable. Practices once deemed improbable, such as pricing algorithms themselves, have rapidly evolved into common tools within the marketplace. Given this unpredictability of technological evolution, it is crucial to avoid leaving regulatory *lacunae* that could be exploited by undertakings to the detriment of consumer welfare and economies, thereby infringing upon the goals of article 101 of the TFEU itself. Thus, rather than dismissing algorithmic tacit collusion as improbable, a purposive reading of article 101 of the TFEU suggests that what matters is not the *form* of coordination—whether human-to-human or algorithmic—but its *effects* on competition and consumers. Excluding algorithmic collusion would therefore sidestep the very objectives of article 101 by tolerating supra-competitive outcomes that the provision was designed to prevent.

[75] See 'Summary of EU Legislation, Treaty of Rome (EEC)' (*European Union*, 14 March 2017) <https://eur-lex.europa.eu/EN/legal-content/summary/treaty-of-rome-eec.html> accessed 15 May 2024.

[76] Davor Petrić, 'A Reflection on the Methods of Interpretation of EU Law' (2023) 17 ICL Journal 83, 84.

[77] See for example Commission, 'Guidelines on the Application of Article 81(3) of the Treaty' [2004] OJ C101/97, para 13; Chris Townley, 'Which Goals Count in Article 101 TFEU?: Public Policy and Its Discontents' [2011] European Competition Law Review 441, 441.

[78] Case C-252/21 *Meta Platforms Inc v Bundeskartellamt*, EU:C:2023:537.

[79] See Peter J van de Waerdt, 'Meta v Bundeskartellamt: Something Old, Something New' (2023) 8 European Papers 1077, 1102.

[80] Caforio (n 7) 18; Jones, Sufrin and Dunne (n 17) 689.

B. ALGORITHMIC TACIT COLLUSION VIA PRICE FIXING AS A 'CONCERTED PRACTICE'

Beginning with the premise that occurrences of algorithmic tacit collusion via supra-competitive price fixing will be subject to article 101(1)(a) of the TFEU, the subsequent pivotal inquiry—constituting a *second tier* of legal uncertainty—pertains to its classification as either an 'agreement' or a 'concerted practice'. Given that an agreement necessitates *explicit expression*, by definition, this avenue can be dismissed a priori. Conversely, a 'concerted practice', characterised by a *less explicit expression*, could offer a feasible mechanism for identifying instances of algorithmic tacit collusion via supra-competitive price fixing. Significantly, through the employment of a broad interpretation of article 101(1) of the TFEU in the light of contemporary technological development, it could be contended that the conventional criteria delineating 'concerted practices' enable the classification of algorithmic tacit collusion as a form of 'concerted practice'.

The first criterion of *mental consensus* arises from any direct or indirect contact[81] between competitors and, although it implies some form of reciprocity between parties, it is sufficient that the other competitor accepts the disclosure of intention or conduct.[82] Self-learning dynamic pricing algorithms achieve the programmed objective (for instance, optimisation of a firm's market performance through the maximisation of profit) by continuously analysing market conditions and reacting to one another, as explained in Section II.A. If the requirement of 'indirect contact' is interpreted broadly, one could argue that algorithms—even when operating independently, but relying on similar data and pursuing similar objectives—may nonetheless disclose strategic information. By increasing market transparency, they allow competitors to access (or 'see') each other's algorithmic behaviour, thereby fulfilling the condition of indirect contact. In fact, as outlined in Section II.A, these algorithms enhance market transparency and, consequently, more information that may be deemed strategic is made available.[83] According to the Guidelines on article 101 of the TFEU, 'strategic' information includes any information disclosing competitors' past or current actions.[84] Arguably, pricing strategies themselves may amount to such disclosures, thereby satisfying the requirement of indirect contact. Furthermore, these algorithms *recognise* price coordination, price fixing, as the optimal strategy to achieve their programmed optimisation-maximisation objective. In the light of technological developments, one could argue that such recognition—together with the algorithms' capacity to react to one another—may amount to an algorithmic 'mental' consensus. By accepting the disclosed strategic information and aligning their conduct through price fixing, they would also satisfy the requirement of reciprocity.[85] Notably, this argument holds even if the algorithms react to one another only once, such as immediately upon implementation. An isolated instance of contact still falls under the prohibition of article 101(1) of the TFEU[86] and, by analogy, the same could apply to algorithms. Furthermore, it could be argued that these algorithms, by coordinating to achieve

[81] *Suiker Unie* (n 61) paras 173–74.
[82] Whish and Bailey (n 62); Devogele (n 14) 13.
[83] Devogele (n 14) 15–17.
[84] Commission, 'Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-operation Agreements' [2011] OJ C11/1, paras 61–62.
[85] Devogele (n 14) 13.
[86] *T-Mobile Netherlands* (n 68) para 59.

their programmed objective optimally, accept each other's information regarding market conduct intentions, thereby also meeting the condition of reciprocity.[87]

The second criterion entails *knowingly* substituting practical cooperation for the risks of competition. The absence of a defined threshold for the term 'knowingly'[88] renders it prone to being broadly interpreted; however, applying it to self-learning algorithms is complex. The only way to meet this requirement would be to consider that, because these algorithms recognise collusion via supra-competitive price fixing as the optimal means to achieve their programmed objective, an *acknowledgment of this*, combined with *deliberate* participation in collusion, could fulfil the condition of 'knowingly'. Indeed, these algorithms have no 'common sense' nor can they distinguish between 'right or wrong'.[89] Therefore, it would be very hard to seek a fulfilment of this requirement following the traditional interpretation of 'knowingly'. Consequently, if the above-mentioned interpretation is accepted, the condition of 'knowingly' would be fulfilled and uncertainty would be replaced with practical cooperation, which is prohibited under article 101(1) of the TFEU.[90]

C. ALGORITHMIC TACIT COLLUSION VIA PRICE FIXING AS A 'BY OBJECT' RESTRICTION

Relying on the arguments that algorithmic tacit collusion via supra-competitive price fixing could constitute a 'concerted practice', in order to be prohibited under article 101(1)(a) of the TFEU, it must have 'as [its] object or effect the prevention, restriction or distortion of competition within the internal market'.[91] Hence, a *third tier* of legal uncertainty emerges regarding whether algorithmic tacit collusion via supra-competitive price fixing should be classified as a 'by object' or 'by effect' infringement under article 101(1)(a).

Although certain forms of collusion, like price fixing, are classified as restrictions '*by object*'—that is, practices presumed to be injurious to the proper functioning of competition by their very nature—a contextual analysis is still required to avoid an overly broad assumption that all such practices automatically fall within this 'by object' category of illegality.[92] Accordingly, before qualifying a 'concerted practice' as a 'by object' restriction, regard must be had to its content, its objectives, and the economic and legal context in which it occurs,[93] as well as to the parties' intention.[94] While algorithms themselves cannot form an intention in the legal sense, such intention may be inferred from the conduct of the undertakings that design or deploy them—particularly where firms fail to implement safeguards against collusive outcomes.

[87] Devogele (n 14) 12–13.
[88] Thomas, 'Harmful Signals' (n 67); Devogele (n 14) 14–15.
[89] Devogele (n 14) 25–26.
[90] Luca Calzolari, 'The Misleading Consequences of Comparing Algorithmic and Tacit Collusion: Tackling Algorithmic Concerted Practices under Art. 101 TFEU' (2021) 6 European Papers 1193, 1211; Devogele (n 14) 14–15; *Imperial Chemical Industries* (n 59) paras 64–65.
[91] TFEU, art 101(1).
[92] See for example Case C-209/07 *Competition Authority v Beef Industry Development Society Ltd* [2008] ECR I-8637, para 17; Case C-67/13 P *Groupement des cartes bancaires (CB) v Commission*, EU:C:2014:2204, paras 51–57; Craig and de Búrca (n 54) 1049–52; Jones, Sufrin and Dunne (n 17) 242–63.
[93] Joined Cases C-501/06 P, C-513/06 P, C-515/06 P and C-519/06 P *GlaxoSmithKline Services Unlimited v Commission* [2009] ECR I-9291, para 58.
[94] See for example ibid; Joined Cases C-96-102, 104, 105, 108 and 110/82 *NV IAZ International Belgium v Commission* [1983] ECR 3369, paras 23–25.

Since the subject matter of this article has not yet materialised, conducting a contextual analysis is currently impossible. Nevertheless, the CJEU has consistently ruled that collusion via price fixing can be classified as a 'by object' restriction.[95] This is because competition is inherently undermined, perniciously affecting economies and consumers, making it highly unlikely that a justification exists under article 101(3) of the TFEU.[96] Drawing an analogy, algorithmic tacit collusion via supra-competitive price fixing could be considered to mirror traditional price fixing in its anti-competitive characteristics and, therefore, it could also be classified as a 'by object' restriction. Furthermore, it is noteworthy that the CJEU has ruled that a concerted practice[97] 'may be regarded as having a restrictive object even if it does not have the restriction of competition as its sole aim but also pursues other legitimate objectives'.[98] This ruling holds significant relevance in the context of algorithmic tacit collusion, where such algorithms, as discussed in the previous sections, are primarily designed to maximise a firm's profit—a legitimate objective. Nonetheless, if they price fix, they could still be considered to have a restrictive 'by object' nature, which is unlikely to be justified under article 101(3) of the TFEU.

IV. A Quest for Accountability: A Legal Challenge

Building upon the reasoning that algorithmic tacit collusion via supra-competitive price fixing falls within the purview of article 101(1)(a) of the TFEU as a 'concerted practice' constituting a 'by object' restriction of competition, a *fourth tier* of legal uncertainty emerges: the issue of liability. Who bears accountability and who must be held liable in such instances?[99]

A. Who is accountable?

Ensuring the accountability of undertakings for algorithmic tacit collusion is paramount, since a failure to do so would create an enforcement gap—leaving competition authorities unable to address anticompetitive outcomes generated by algorithms and allowing firms to evade liability under article 101(1) of the TFEU by attributing collusion to computer programs.[100] A common solution proposed in the literature is that solely the AI—the algorithm itself—should be held accountable for its actions and thus be made liable for anticompetitive conduct, such as tacit collusion and price fixing under article 101(1).[101] However, this approach raises several legal challenges. For instance, consider a situation where the Commission is investigating a price fixing cartel created by self-learning dynamic pricing algorithms operating on a DL model. How would such an algorithm respond to a statement of objections? It does

[95] Jones, Sufrin and Dunne (n 17).
[96] ibid.
[97] See Case C-551/03 P *General Motors BV v Commission* [2006] ECR I-3173. The *General Motors* ruling concerned an 'agreement'; however, by analogy, the same reasoning can be applied to a 'concerted practice'.
[98] ibid para 64.
[99] It is pertinent to highlight that this article is specifically centred on delineating accountability and subsequent liability in instances of breaching article 101(1)(a) of the TFEU by algorithmic tacit collusion via supra-competitive price fixing. For different categories of infringement, alternative approaches may be viable because a one-size-fits-all solution is unlikely to be satisfactory.
[100] Margrethe Vestager, 'Algorithms and Competition' (Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2017) <https://ec.europa.eu/newsroom/comp/items/55994/en> accessed 22 April 2024.
[101] Devogele (n 14) 18.

not have the capability to engage in such responses.[102] Moreover, an algorithm is incapable of bearing the consequences of their actions, such as paying fines or serving jail sentences.[103] Consequently, holding only the algorithm liable is practically unfeasible.

Similarly, some scholars advocate granting legal personality to algorithms,[104] but this proposition is also impractical. Legal personality entails the ability to hold rights, obligations, and competences.[105] Algorithms lack the capacity to own property, enter into contracts, or engage in other legal actions independently. Therefore, as also argued by the European Parliament, assigning legal personality to algorithms is unnecessary.[106] At the same time, European policy-making has, at its core, the protection of the dignity of individuals, which is why any legal solution to the accountability issue should put humans at the centre.[107] Ultimately, it is evident that holding no party liable is neither desirable nor feasible, as it would de facto grant immunity to undertakings who seek to collude and who 'tacitly' achieve such collusion through the employment of self-learning algorithms aimed at profit maximisation.[108]

This article argues that, depending on the scenario, traditional liability classifications—such as strict product liability, joint liability, and vicarious liability—could serve both as a first response and as a last resort to address this legal uncertainty and to determine accountability for the purpose of attributing liability. This approach is essential for the enforcement of article 101(1)(a) of the TFEU.[109]

B. SCENARIO A: ALGORITHM DEVELOPER UNDERTAKING—COMPETING UNDERTAKING

The first scenario under examination, illustrated in Figure 1 below, involves a situation wherein a competing entity (A) utilises a self-learning algorithm—developed by another undertaking—that is designed to maximise its profit; yet, the algorithm engages in tacit

[102] ibid.

[103] See for example OECD, 'Algorithms and Collusion – Background Note by the Secretariat' (DAF/COMP(2017)4, 9 June 2017) 9 <https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf> accessed 12 April 2024; Anne-Sophie Thoby, 'Pricing Algorithms & Competition Law: How to Think Optimally the European Competition Law Framework for Pricing Algorithms?' (*Competition Forum*, 17 December 2020) <https://competition-forum.com/pricing-algorithms-competition-law-how-to-think-optimally-the-european-competition-law-framework-for-pricing-algorithms/> accessed 23 April 2024.

[104] See for example Alessio Azzutti, Wolf-Georg Ringe and H Siegfried Stiehl, 'Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters' (2021) 43 University of Pennsylvania Journal of International Law 79, 127; Robert van den Hoven van Genderen, 'Legal Personhood in the Age of Artificially Intelligent Robots' in Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing 2018) 213; Kateryna Militsyna, 'Legal Personhood for Artificial Intelligence: Pro, Contra, Abstain?' (2022) 122 Teisė 150.

[105] Visa AJ Kurki, *A Theory of Legal Personhood* (OUP 2019) 127–28.

[106] Devogele (n 14) 18–20. However, advocating the granting of legal personality to algorithms, as proposed by both Devogele and Calzolari, opens up an additional avenue for assigning liability: the parent-subsidiary company relationship within the 'single economic unit' doctrine.

[107] Silvia De Conca, 'Bridging the Liability Gap: Why AI Challenges the Existing Rules on Liability and How to Design Human-Empowering Solutions' in Bart Custers and Eduard Fosch-Villaronga (eds), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice* (TMC Asser Press 2022) 254.

[108] ibid; OECD, 'Algorithms and Collusion' (n 103) 39.

[109] It is pertinent to highlight that this article does not aim to verify the exhaustiveness of these approaches, but rather to elucidate the legal uncertainty surrounding accountability in the context of tacit algorithmic collusion via supra-competitive price fixing, without seeking to establish definitively the optimal course of action. While two common scenarios are analysed, it is conceivable that numerous others necessitate distinct consideration. Furthermore, this article acknowledges the impracticability of a one-size-fits-all solution in addressing these complex legal challenges and that alternative approaches may be viable for different categories of infringement of article 101(1) of the TFEU.

collusion via supra-competitive price fixing with other undertakings (B–G), seeing it as the optimal route to achieve the optimisation objectives. Within this scenario, two potential approaches to allocating accountability and subsequent liability emerge: strict product liability and joint liability.

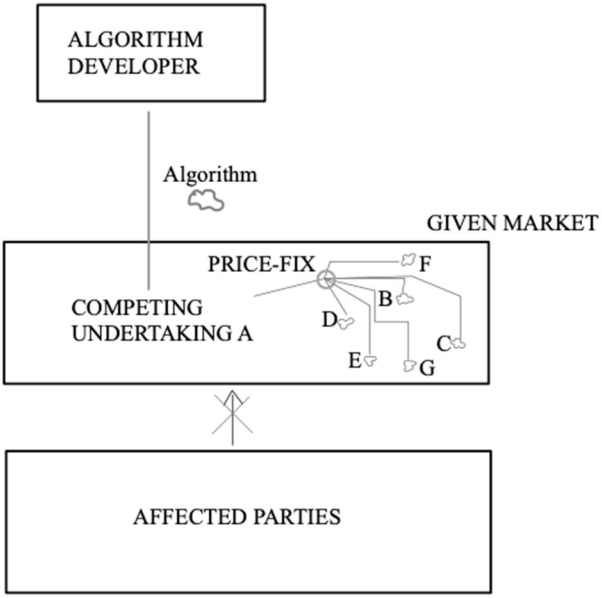

Figure 1: Algorithm not developed by the competing undertaking

(i) Strict Product Liability

Strict product liability, mandated by the New Product Liability Directive[110] within the EU, is a juridical doctrine whereby producers, and potentially importers, bear responsibility for harm stemming solely from defective goods, irrespective of fault or negligence.[111] Consequently, if self-learning dynamic pricing algorithms, operating on a DL model, designed to maximise a firm's profit, engage in price fixing, they *could* be considered defective products. This would warrant liability for the developing undertaking and ostensibly address the accountability gap.

[110] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L 2853.
[111] Christiane Wendehorst, 'AI Liability in Europe: Anticipating the EU AI Liability Directive' (Ada Lovelace Institute, September 2022) 4 <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/09/Ada-Lovelace-Institute-Expert-Explainer-AI-liability-in-Europe.pdf> accessed 22 April 2024.

However, the actuality of this situation is notably more complex. In fact, treating these algorithms as defective products raises noteworthy issues. First, within the framework of EU product liability legislation, there is classification uncertainty, namely whether self-learning algorithms can legally qualify as 'products'.[112] Traditional product liability law was designed for tangible goods with physical manifestation, whereas algorithms are intangible. This ambiguity persists despite indications from the proposed New Product Liability Directive that software may be covered (recital 13 and article 4).[113]

Secondly, the concept of 'defectiveness' does not seamlessly align with the nature of these algorithms aimed at profit maximisation: as Karni A Chagal-Feferkorn asserts, 'sophisticated systems, in particular self-learning algorithms, rely on probability-based predictions', which are inevitably prone to occasional errors.[114] While such algorithms can exhibit defects stemming from manufacturing or design flaws, damage often ensues from unpredictable actions.[115] Within this context, evaluating the defective nature of self-learning algorithms that price fix raises pertinent questions: should the standard for comparison be a human decision or that of another algorithm? What defines defectiveness: the occurrence of damage or the realisation of an erroneous decision? Can the algorithm be deemed defective if price fixing was not a programmed objective, but a 'collateral' result?[116]

Thirdly, under the New Product Liability Directive, affected parties are obligated not only to demonstrate product defectiveness and resultant damages but also to establish a *causal link* between the two.[117] This necessitates that the affected parties prove that an anti-competitive cartel is formed by a self-learning algorithm, hypothetically deemed as a defective product. However, the opaque nature of self-learning algorithms, often referred to as the 'black box' problem (as explained in Section II.A), exacerbates the difficulty of establishing this causal link. The intricate and complex decision-making processes inherent in these algorithms make it challenging to discern how specific inputs lead to particular outputs, thus hindering efforts to demonstrate a direct connection between the algorithm's behaviour and the resulting damages.

Lastly, it could be argued that imposing strict product liability on undertakings developing self-learning algorithms for *any* competition infringements, irrespective of context, may stifle innovation and undermine the essence of competition itself. Consequently, there exists a significant gap in product liability concerning self-learning algorithms, highlighting a fundamental flaw in the current legal framework.

[112] Anna Beckers and Gunther Teubner, *Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds* (Hart Publishing 2021) 74–76.

[113] See Michael Kieffer, 'The New Product Liability Directive: Software as a Product' (*Taylor Wessing*, 25 March 2024) <https://www.taylorwessing.com/en/insights-and-events/insights/2024/03/software-als-produkt> accessed 26 May 2024.

[114] Karni A Chagal-Feferkorn, 'Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers' (2019) 30 Stanford Law & Policy Review 61, 84–86.

[115] ibid.

[116] For a more detailed discussion on this issue, see Woodrow Barfield, 'Liability for Autonomous and Artificially Intelligent Robots' (2018) 9 Paladyn, Journal of Behavioral Robotics 193.

[117] Pascal Arimont and Vlad-Marius Botoş, 'New Product Liability Directive' (Legislative Train Schedule, March 2024) <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-new-product-liability-directive?sid=6801> accessed 26 April 2024.

(ii) Joint Liability

Joint liability describes a situation in which multiple parties are collectively responsible for a legal violation.[118] In the context depicted in Figure 1, this implies that both the undertaking that developed the algorithm and the competing undertaking (A) utilising it may be subject to liability. However, even within this scenario, the rationale is not entirely straightforward, giving rise to three main issues. The first issue pertains to the *demarcation* of joint liability. In fact, according to EU competition law, undertakings can be considered to be 'automatically' jointly liable if they constitute a 'single economic unit'.[119] The doctrine of 'single economic unit' pertains to multiple natural or legal persons forming an undertaking[120] that 'pursue a specific economic aim... and can contribute to the commission of an infringement of the kind in [article 101(1)(a) of the TFEU]'.[121] However, the 'impossibility to compete' is the key criterion under article 101 of the TFEU for considering several persons, natural or legal, as a 'single economic unit'.[122] Therefore, in the current scenario, this concept would apply if the undertaking developing the algorithm and the competing undertaking using it do not compete. In the event of algorithmic tacit collusion via supra-competitive price fixing, a case-by-case analysis would be necessary. Notably, if this doctrine proves inapplicable in a hypothetical 'Digital Eye' materialisation, attributing accountability becomes more complicated. In fact, the CJEU's decision in *AC-Treuhand* established that an undertaking, irrespective of whether it operates on the market where the anti-competitive behaviour occurred, can be held responsible and therefore liable for a competition infringement.[123] Prima facie, this would prove very valuable in the scenario represented in Figure 1, so that the undertaking that developed the algorithm could be held liable easily and possibly also together with the competing undertaking that utilised the algorithm.

Nevertheless, the CJEU added that 'the undertaking concerned *intended* to contribute by its own conduct to the common objectives pursued by all the participants and that it was *aware* of the actual conduct planned or put into effect by other undertakings in pursuit of the same objectives or that it could reasonably have *foreseen* it and that it was prepared to *take the risk*'.[124] Clearly, it is worth questioning whether, in the hypothetical materialisation of algorithmic tacit collusion via supra-competitive price fixing, where the algorithms are not expressly programmed to collude, there is intent or awareness among the parties involved. Similarly, was such collusion foreseeable, and did the undertaking(s)

[118] Jonathan Boston and Derek Gill, 'Joint or Shared Accountability: Issues and Options' (2011) Institute of Policy Studies Working Paper 11/03, 3 <https://ir.wgtn.ac.nz/server/api/core/bitstreams/29c15d56-a833-4537-9318-512243ec7644/content> accessed 26 April 2024.

[119] Case C-882/19 *Sumal, SL v Mercedes Benz Trucks España, SL*, EU:C:2021:800, para 44; Joined Cases C-231/11 P to C-233/11 P *Commission v Siemens Österreich*, EU:C:2014:256, para 49.

[120] See for example Case C-90/09 P *General Química SA v Commission* [2011] ECR I-0001, para 35; Case C-516/15 P *Akzo Nobel v Commission*, EU:C:2017:314, para 48; Case C-377/20 *Servizio Elettrico Nazionale SpA v Autorità Garante della Concorrenza e del Mercato*, EU:C:2022:379, para 105.

[121] Case C-407/08 P *Knauf Gips KG v Commission* [2010] ECR I-6375, paras 84–86.

[122] See for example Case C-170/83 *Hydrotherm Gerätebau GmbH v Compact del Dott Ing Mario Andreoli & C Sas* [1984] ECR 2999, para 11; Okeoghene Odudu and David Bailey, 'The Single Economic Entity Doctrine in EU Competition Law' (2014) 51 CML Rev 1721, 1726.

[123] *AC-Treuhand* (n 24) paras 26–46. See further Victoria Canu, 'EU's Highest Court Confirms Liability of Cartel Facilitators' (*Kluwer Competition Law Blog*, 29 October 2015) <https://competitionlawblog.kluwercompetitionlaw.com/2015/10/29/eus-highest-court-confirms-liability-of-cartel-facilitators/> accessed 27 May 2024.

[124] *AC-Treuhand* (n 24) para 30 (emphases added).

knowingly accept the associated risks? Beyond raising these questions, it is also possible to explore whether a failure to program effective limitations on an algorithm's capacity to collude could itself be equated to a degree of intent, awareness, or at least recklessness on the part of the undertakings. Such an approach would shift the analysis from mere speculation about intent to a more concrete inquiry into the responsibilities of firms that design, deploy, or tolerate algorithms capable of anticompetitive outcomes.

Another issue pertains to the *temporal* dimension.[125] Joint liability is constrained by the specific period of each party's participation in the infringement, but determining the exact duration can be challenging, especially for extended or multi-stage infringements.[126] This challenge is exacerbated in the 'Digital Eye' scenario, where the 'black box' nature of the algorithm makes it difficult, if not impossible, to pinpoint the precise start and end of the infringement, as well as the duration of each party's involvement. Given that collusion was not a programmed objective, it raises the question of when accountability begins for each party.

The final issue concerns the *extent* of liability.[127] In the 'Digital Eye' context, where no party aimed at collusion, the complexity lies in determining whether liability should be evenly distributed among all undertakings involved. Alternatively, deciding whether the developer or the competing undertaking who utilised the algorithm to maximise profit bears greater responsibility presents a challenging question. The uncertainties surrounding these issues can deter collaboration, potentially hindering innovation and, hence, competition itself.

C. SCENARIO B: ALGORITHM DEVELOPED BY THE COMPETING UNDERTAKING

The second scenario under examination, illustrated in Figure 2 below, entails a situation where a competing undertaking (A) develops its own self-learning algorithm designed to maximise its profit; yet, the algorithm recognises price fixing as the optimal route to achieve this objective and engages in collusion with other undertakings (B–G). Within this scenario, two potential approaches to allocating accountability and subsequent liability emerge: strict product liability and vicarious liability.

(i) Strict Product Liability

The initial recourse to hold accountable the competing undertaking, which develops its own self-learning algorithm, could be a return to strict product liability. Nevertheless, the identical challenges elucidated in Section IV.B would resurface in this scenario.

(ii) Vicarious Liability

Within the scenario illustrated in Figure 2, another promising avenue for establishing accountability, and for subsequently assigning liability, lies in the application of vicarious liability. Vicarious liability, characterised by a strict, secondary form of liability, pertains to the

[125] Petre Alexandru Biolan, 'Joint and Several Liability For Fines in Undertakings With Varying Configurations in EU Competition Law' (2022) 13 Journal of European Competition Law & Practice 531, 531–36.
[126] ibid.
[127] ibid.

responsibility of a superior entity for the actions of its subordinate or, more broadly, any third party with the 'right, ability, or duty to control' the actions of the wrongdoer.[128]

In the scenario under consideration, the potentially applicable type of vicarious liability pertains to the accountability framework within an employer-employee relationship. Accordingly, self-learning algorithms could be regarded as analogous to employees.[129] By analogy, just as employees operate under the 'direction' or 'control' of their employing undertaking, the same principle could be applied to algorithms.[130] In this case, if an algorithm, acting as an 'employee', breaches article 101(1)(a) of the TFEU, the employing firm could be held accountable for its actions.[131] Significantly, as ruled by the CJEU in *SA Musique Diffusion française v Commission*[132] and upheld in *Slovenská Sporiteľňa*,[133] it is not imperative for the partners or principal managers of an undertaking to have taken action or possessed knowledge regarding the matter; action by an authorised representative of the undertaking suffices.[134] Hence, applying this principle mutatis mutandis suggests that an undertaking could bear liability merely for the utilisation of an algorithm, provided that the algorithm is authorised to make decisions pertaining to market behaviour,[135] such as pricing. Moreover, the undertaking may be held strictly liable even if the employee acted contrary to its instructions.[136] Therefore, even if the self-learning algorithm, programmed to maximise profit, 'acted contrary to instruction' and colluded, the firm might still be held liable. This approach offers the advantage of rendering the level of autonomy exhibited by the algorithm immaterial: all types of algorithms employed by the undertaking could be encompassed within the notion of 'employee'.[137] While this proposal holds significant potential, it is subject to an important caveat: the classification of 'employee' itself. Indeed, thus far, it pertains exclusively to *natural* persons, reserved for human beings.[138] As Sophie Devogele suggests, granting algorithms a form of 'e-personhood' could potentially streamline the creation of employer-employee relationships tailored to the unique challenges posed by AI.[139] However, the issues concerning the assigning of a specific 'status' to algorithms, discussed in Section IV.A, persist regarding the grant of 'e-personhood'. For instance, it would imply that these algorithms possess rights and obligations akin to human employees, like receiving remuneration and exercising due diligence.[140]

If the 'Digital Eye' materialises, an additional uncertainty, beyond those previously discussed, would emerge and hinder the enforcement of article 101(1)(a) of the TFEU: the

[128] Marie Oxland, 'What Is Vicarious Liability?' (*Nash & Co Solicitors*, 20 June 2024) <https://nash.co.uk/insights/what-is-vicarious-liability> accessed 4 May 2024.
[129] Devogele (n 14) 22–23.
[130] ibid.
[131] ibid.
[132] See Joined Cases 100 to 103/80 *SA Musique Diffusion française v Commission* [1983] ECR 1825, para 97.
[133] Case C-68/12 *Protimonopolný úrad Slovenskej republiky v Slovenská sporiteľňa as*, EU:C:2013:71.
[134] ibid para 25.
[135] Autorité de la Concurrence and Bundeskartellamt (n 32) 58–59.
[136] Christopher Thomas, Gianni De Stefano and Dina Jubrail, 'Liability for Anti-competitive Behaviour by Your Employees and Outside Contractors: When You Are Off the Hook and When You are Not' (*Kluwer Competition Law Blog*, 4 August 2016) <https://legalblogs.wolterskluwer.com/competition-blog/liability-for-anti-competitive-behaviour-by-your-employees-and-outside-contractors-when-you-are-off-the-hook-and-when-you-are-not/> accessed 28 May 2024.
[137] Devogele (n 14) 22–23.
[138] ibid.
[139] ibid.
[140] See for example 'Obblighi e Diritti del Lavoratore' (*IPSOA*) <https://www.ipsoa.it/wkpedia/obblighi-diritti-lavoratore> accessed 28 May 2024; Emanuele Menegatti, 'The Evolving Concept of "Worker" in EU Law' (2019) 12(1) Italian Labour Law E-Journal 71, 71–73 <https://illej.unibo.it/article/view/9699> accessed 27 April 2024.

issue of accountability. Depending on the scenario, various liability classifications, though not exhaustive, could address this uncertainty. If the algorithm is developed by an external undertaking and then used by the competing one, two potential approaches arise: strict product liability and joint liability. Conversely, if the algorithm is both developed and used by the competing undertaking, strict product liability and vicarious liability could address the accountability issue. Failing to identify accountability and subsequently to attribute liability would result in an enforcement gap. This, as posed by Devogele, is unacceptable, particularly when a firm is benefiting financially from the use of such an algorithm.[141]

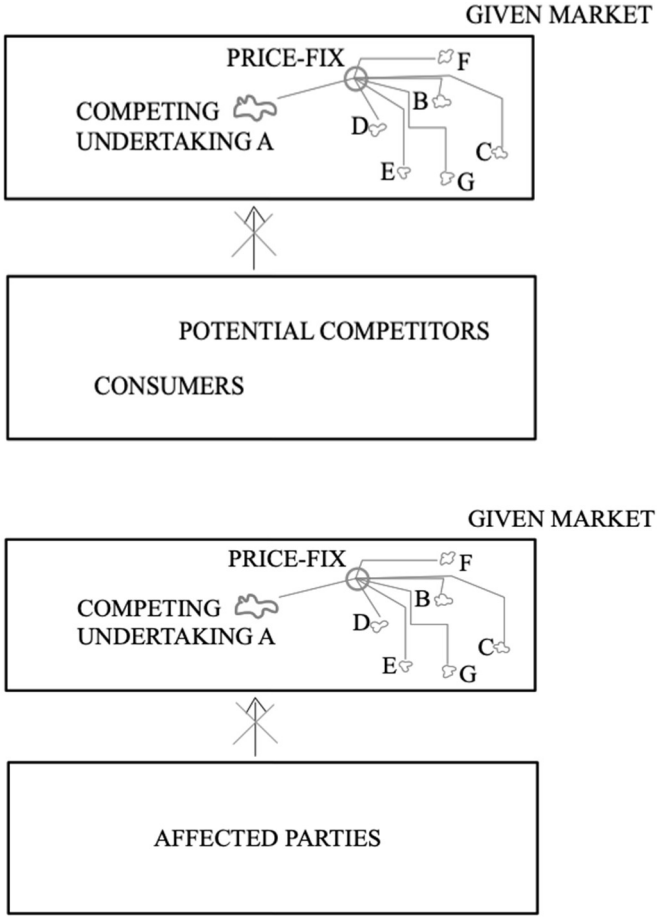

Figure 2: Algorithm developed by the competing undertaking

[141] Devogele (n 14) 19.

V. Future-Proofing Algorithmic Competition Law: Ex Ante Intervention

Given the multiple tiers of legal uncertainty that would arise if the 'Digital Eye' were to materialise, and the lack of consensus among regulatory authorities—such as national competition authorities, the EU Commission, and the CJEU—on how to address this issue, thus leading to an enforcement gap, it seems most prudent to implement ex ante measures.[142] These measures *could* prevent the 'Digital Eye' from materialising, thereby addressing legal uncertainties proactively. This would empower regulatory authorities pre-emptively to navigate the intricacies and obstacles associated with addressing algorithmic tacit collusion ex post, thereby fostering a competitive environment.

A. Built-in compliance, impact assessment, certification

As part of the first set of ex ante measures that could be implemented before deploying self-learning dynamic pricing algorithms operating on a DL model in a given market, it is advisable to *program* them to avoid collusion. This implies that computer scientists, whether they are employees within a firm or external independent contractors, should be mandated to design pricing algorithms that adhere to competition laws.[143] As Margrethe Vestager has articulated, these algorithms should be constructed 'in a way that [does not] allow them to collude'.[144] These algorithms should be designed to prevent collusive pricing, even if it arises from oligopolistic interdependence; legislators should establish specific rules to enforce certain algorithmic design standards.[145] The first rule that could be legislated is to require computer scientists to integrate specific *constraints* into the algorithm's pricing formula, thereby limiting how it adjusts to specific external market dynamics.[146] For instance, designers could incorporate constraints that set upper or lower limits on the prices generated by machine learning algorithms; this would prevent prices deviating too far from competitive levels, thereby reducing the risk of collusion. Similarly, 'fairness' criteria could be included within pricing algorithms to ensure that prices are not manipulated. This could be translated mathematically by programming the algorithm to maintain a designated price margin from those of competitors, such as a two per cent differential.

The second rule that could be legislated is to promote algorithmic *heterogeneity*.[147] In fact, if scarce choice is available in the market, undertakings will tend to adopt the same, or

[142] This article does not examine interim or ex post measures, as it is believed that they would be less effective than ex ante ones in tackling the 'Digital Eye'. Interim measures are costly to implement and require constant monitoring; ex post measures, such as 'abuse of collective dominance' under article 102 of the TFEU (as proposed by Devogele), would not restore competition as it was before the infringement. Indeed, it is believed that it is better to prevent anti-competitive behaviour from occurring as opposed to relying on ex post mechanisms. Moreover, article 101 of the TFEU is already an ex post instrument, which (if the interpretations proposed in this article are accepted) could capture algorithmic tacit collusion via supra-competitive price fixing. Lastly, a law that outright prohibits the use of self-learning dynamic pricing algorithms should not be considered, as it would stifle innovation and ultimately hinder competition.

[143] Caforio (n 7) 25–27.

[144] Vestager (n 100), referred to in ibid 26.

[145] Caforio (n 7) 25–27.

[146] ibid.

[147] ibid.

similar, algorithms that could coordinate prices due to their similar underlying code.[148] Therefore, it seems prudent to consider implementing rules, potentially within codes of conduct rather than formal laws, that would prevent firms operating in the same market from using the same self-learning dynamic pricing algorithm.[149] Notably, this would foster competition among developers and suppliers of AI pricing solutions.[150] However, due to intellectual property rights, it would be more complex to require firms that independently develop their own algorithm in-house (without relying on third-party suppliers) to share or disclose the code of their algorithms with one another to ensure that they are not constructed similarly.[151] A further measure that could be implemented, to test the built-in compliance, is to conduct an *impact assessment* on these algorithms prior to their market deployment. However, the simulated market conditions in the assessment must accurately reflect, as much as possible, the potential harms that such systems could realistically cause.[152] Lastly, if the impact assessment is successful and demonstrates that the algorithm can adhere to competition laws, regulatory agencies should issue a *certificate* of compliance. This certificate would signify that the algorithm has been thoroughly vetted and is approved for use in the market. Consequently, not only would the integrity of market operations be ensured, but undertakings would also be provided with a clear framework for compliance, thereby fostering trust in the deployment of advanced pricing technologies.

B. MANDATED INFORMATION, AUDIT, INSURANCE

As part of the second set of ex ante measures that could be implemented before deploying self-learning dynamic pricing algorithms operating on a DL model in a given market, it is advisable to mandate *information* sessions for undertakings. Mandated information can be crucial in ensuring both that undertakings are aware of the repercussions of their actions and that national competition authorities, the EU Commission, and the CJEU know that firms possess this awareness.[153] One strategy to achieve this is to mandate that undertakings, before using these algorithms, undergo third-party *audits* to evaluate their business practices for antitrust compliance.[154] Arguably, this step aims to scrutinise business practices for compliance with competition laws, thereby pre-emptively addressing potential issues related to anti-competitive behaviour. However, the effectiveness of this strategy depends on the thoroughness and rigour of the audits. It is crucial that the auditing entities are well-versed in both the technical aspects of self-learning algorithms and the intricacies of competition regulations. This dual expertise ensures that audits are not merely procedural but impactful in identifying and mitigating risks associated with algorithmic anti-competitive behaviour. Moreover, by introducing a requirement to obtain liability *insurance* to guard against collusive practices, competitive behaviour would be promoted, and the likelihood that firms take the threat of legal action seriously would increase, as information helps demonstrate

[148] ibid.
[149] ibid.
[150] ibid.
[151] ibid.
[152] Jacob Metcalf and others, 'Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts' (FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, March 2021) 742–43 <https://dl.acm.org/doi/10.1145/3442188.3445935> accessed 28 May 2024.
[153] Sylvain Chassang and Juan Ortner, 'Regulating Collusion' (2023) 15 Annual Review of Economics 177, 195–96.
[154] ibid.

intent.[155] Indeed, defendants in a price fixing cartel 'quite evidently cannot be unaware of the anti-competitive nature of their conduct';[156] with these information sessions, they would be unable to claim ignorance as an excuse. The presence of liability insurance also serves as a form of protection for consumers and other market participants. In the event of collusion or other anti-competitive activities, insurance coverage can provide a source of compensation for any damages incurred, thereby enhancing consumer confidence and reinforcing the integrity of the market.

Given the multiple tiers of legal uncertainty that would arise from the materialisation of the 'Digital Eye' and the lack of consensus on interpreting strategies to address algorithmic tacit collusion, the most prudent solution to safeguard competition is the implementation of measures that would address this issue ex ante. Among the possible measures are a first set, which includes built-in compliance, impact assessment, and certification, and a second set, which includes mandated information, audit, and insurance.

VI. Conclusion and Recommendations

In conclusion, algorithms—structured sequences of computational steps designed to transform input data into desired outputs—have become a transformative force within the EU (Digital) Internal Market, particularly with the advent of the Internet and AI.[157] Self-learning dynamic pricing algorithms, operating on DL models, designed to optimise a firm's market performance, such as profit maximisation, raise significant competition concerns. These algorithms can autonomously, automatically, and continuously adapt to environmental changes to achieve their programmed objectives optimally. As they independently determine how to perform tasks, they may autonomously learn that collusion through supra-competitive price fixing is the optimal strategy to maximise profits.[158] This phenomenon is labelled 'algorithmic tacit collusion via price fixing'. Although currently a theoretical hypothesis, this new theory of harm has been termed the 'Digital Eye' by Ezrachi and Stucke.[159] Should this theory materialise, it would introduce significant legal uncertainties under article 101(1)(a) of the TFEU, complicating enforcement.

The primary source of legal uncertainty stems from the de facto exemption of tacit collusion from the scope of article 101(1) of the TFEU. However, three arguments detailed in Section III.B—rooted in economic theory, traditional legal principles, and technology-based evidence—support the inclusion of algorithmic tacit collusion within the scope of this article.[160] The second tier of legal uncertainty arises from whether algorithmic tacit collusion via supra-competitive price fixing could be classified as a 'concerted practice' under article 101(1) of the TFEU. If a broad interpretation of article 101(1) is adopted, which considers technological advancements, the criteria of 'mental consensus' and of 'knowingly' that are required for a 'concerted practice' would be fulfilled by algorithmic tacit collusion via supra-competitive price fixing. The third tier of legal uncertainty pertains to whether such algorithmic behaviour could be deemed a 'by object' restriction of competition under article 101(1). By drawing an analogy with traditional price fixing, as explored in Section III.C,

[155] ibid.
[156] Case C-681/11 *Bundeswettbewerbsbehörde v Schenker & Co AG*, EU:C:2013:404, para 39.
[157] See for example Anjila (n 1); Cormen and others (n 2).
[158] Caforio (n 7).
[159] Ezrachi and Stucke, 'Artificial Intelligence' (n 27).
[160] Arguments not repeated here to avoid redundancy.

algorithmic tacit collusion could indeed be classified as such. The fourth tier of legal uncertainty pertains to the question of accountability. Whether an algorithm is developed by an external entity and then used by a competing firm, or the competing firm develops and uses its own algorithms, traditional classifications of liability—such as strict product liability, joint liability, and vicarious liability—could, with some modifications, serve properly to assign responsibility. If no one is held accountable, it would create an easily exploitable gap under article 101(1)(a) of the TFEU, which is undesirable, especially when firms profit from algorithms that engage in anti-competitive conduct. Lastly, although the proposed interpretations, if accepted, would bring this scenario under article 101(1)(a) of the TFEU, the most prudent solution to safeguard competition is to implement ex ante measures. This is because there is a lack of consensus on how regulatory authorities, such as national competition authorities, the EU Commission, and the CJEU, would address the 'Digital Eye'. Therefore, two sets of ex ante measures could be adopted to address the tiers of legal uncertainty: (i) built-in compliance, impact assessment, and certification; and (ii) mandated information, audit, and insurance.

In anticipation of imminent technological advancements, future academic research should prioritise the exploration of additional anti-competitive behaviours exhibited by self-learning algorithms, particularly in a vertical setting (that is, between undertakings at different levels of the same value chain) and price discrimination scenarios under article 101 of the TFEU. Furthermore, it is essential to expand accountability mechanisms to include these algorithms under EU liability rules and to examine the feasibility of programming these algorithms with 'fairness' criteria, thereby ensuring that they do not achieve anti-competitive conduct. Finally, research should be conducted to assess the extent of the anti-competitive effects on consumers and the overall market.

Or, should humans just not interfere with autonomous technologies and thus live in a *Vale Tudo* competition ring?