Competition law in the age of AI: Confronting algorithmic collusion in the smart economy

Chen LI,
PhD in Law, Southwest University of Science and Technology, Centre of Latin American and Caribbean Studies, Mianyang, China
yb77204@um.edu.mo

Ina VIRTOSU,
PhD in EU Law, University of Macau, SAR Macau, China
yb67199@connect.um.edu.mo, ivirtosu3@gmail.com

Abstract
AI-driven pricing has become vital in the smart economy, boosted by advancements in IoT, AI, and big data. While robots and AI systems enhance efficiency and drive innovation across digital commerce platforms, they also raise competition law concerns. Algorithmic collusion is a prime example, as autonomous algorithms can independently coordinate market behaviour, challenging traditional liability frameworks. Though competition laws in regions like the EU, US, and China generally prohibit algorithmic collusion, the complex structures of these algorithms make it difficult to pinpoint responsible parties and assign liability accurately. This paper explores these complexities and examines algorithmic collusion's implications for liability attribution through a comparative lens. While EU case law provides some regulatory guidance, it often falls short in addressing the unique nature of algorithmic collusion. China's approach is more restrictive, at times overlooking the autonomy of advanced AI systems. Given its distinct characteristics, algorithmic collusion requires a regulatory approach that differs from traditional collusion, particularly regarding liability. Additionally, this paper argues for the potential special liability of AI designers, who, given their expertise and control over AI, may need to adhere to higher ethical standards. These considerations suggest a need for regulation that both safeguards fair competition and fosters innovation in the evolving digital economy.

Keywords: pricing AI, liability, regulation, ethical AI.

1. Introduction
The smart economy represents a transformative evolution of economic systems, driven by advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data. These technologies enable seamless connectivity between devices, facilitate data-driven decision-making, enhance automation, fundamentally reshaping industries and consumer interactions [57]. In this ecosystem, IoT devices collect real-time data, AI processes it into actionable insights, and big data analytics optimize processes across sectors. Together, these elements power a digital economy that promises efficiency, innovation, and growth on a scale previously unimaginable [2]. IoT, AI and other advanced technologies are reshaping various fields within the digital economy [3]. In healthcare AI refines diagnostic processes, personalizes treatment plans, supports drug discovery and enhances pandemic management [60, 61]. In finance, it powers fraud detection, exchange rate forecasting [6], algorithmic trading, and personalized financial planning. In education, AI-driven platforms enable adaptive learning, automate administrative tasks, and enhance accessibility. E-commerce benefits through personalized recommendations, inventory optimization, and chatbots for customer engagement. Manufacturing is undergoing a transformation with smart factories utilizing predictive maintenance and robotics. In

transportation and logistics, AI optimizes route planning, facilitates autonomous driving, and improves supply chain management. Moreover, smart cities leverage these technologies for traffic management [7], energy efficiency, urban planning [8], and waste management [9], while agriculture benefits from precision farming, crop monitoring, and automated harvesting [10]. These technologies are also driving innovations in entertainment, with AI-generated content and immersive experiences, and energy, optimizing renewable energy management and distribution [11].

Despite these advancements, the smart economy introduces significant challenges, particularly in maintaining fair competition. The widespread adoption of AI-driven tools, including pricing algorithms and supply chain optimizers, raises concerns about anticompetitive practices. These tools, while designed to maximize efficiency and profit, have the potential to unintentionally or deliberately manipulate markets. For example, AI systems may identify patterns that enable coordinated behaviors, such as price setting, that can harm consumer welfare and market fairness [12]. This highlights the growing need for competition laws to adapt to technological advancements.

One of the most pressing challenges in this context is algorithmic collusion, where AI algorithms independently align pricing or other market behaviors without explicit human agreement. Unlike traditional collusion, which typically involves human actors forming cartels, algorithmic collusion can emerge autonomously, making it difficult to detect and regulate. This phenomenon is particularly significant in highly digitalized markets, where algorithms can rapidly process vast amounts of data and respond in real time. Algorithmic collusion poses a dual threat: it undermines the principles of fair competition and complicates the enforcement of existing competition laws, which were largely designed for human-centric coordination [13].

Addressing algorithmic collusion requires a nuanced understanding of the smart economy's technological underpinnings and their interaction with legal frameworks. As jurisdictions grapple with these complexities, this paper explores how competition law can evolve to address these challenges while fostering innovation.

2. Understanding algorithmic collusion

2.1. Definition of algorithm

Algorithms have diverse meanings depending on their application, spanning from self-driving cars and automated medical devices to pricing mechanisms in digital commerce platforms. The OECD, in its report "Algorithms and collusion", provides a general definition: "a sequence of rules performed in an exact order to carry out a specific task" [14]. While this definition is broad, algorithmic collusion requires a more specific understanding, focusing on algorithms designed to set prices autonomously or as instructed by undertakings.

Li Chen, in "Algorithmic collusion and Artificial Intelligence: From the perspective of EU competition law," refines this concept by defining an algorithm as "a computer program for calculating a price." This definition underscores the functional nature of algorithms as programmable tools, distinct from static instructions or manual processes. Moreover,

algorithms are not only developed for internal use but are also commercialized as products or services, enabling their deployment by third parties in various market settings [15].

From a technical perspective, algorithms can also be described as "procedures for solving mathematical problems in a finite number of steps," a concept aligned with logistica numeralis, the principle of numerical computation. This highlights whether an algorithm takes the form of a basic middle-school equation or a sophisticated Q-learning algorithm used in reinforcement learning, its fundamental essence remains a method of calculation [15, 16].

The UK's Competition and Markets Authority (CMA) broadens this view, defining an algorithm as "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values as output" [17]. This inclusive definition covers various types of algorithms, such as monitoring algorithms that track market trends, parallel algorithms designed for real-time operations, and signaling algorithms used for indirect communication between competitors. These diverse algorithm types, as outlined in the OECD report "Algorithms and collusion: Competition policy in the Digital Age," all fall under the umbrella of pricing mechanisms [18].

For pricing algorithms to function effectively, they must be coded as computer programs, as static mathematical formulas alone cannot execute dynamic price-fixing tasks. Commercialization adds another layer of complexity, as it allows these tools to be sold or licensed, enabling other entities to use them for collusive purposes. A report by the Competition Authority of Portugal, "Ecosystems, big data, and algorithms," revealed that 37% of surveyed enterprises admitted to using algorithms for pricing, demonstrating the widespread availability and potential misuse of these tools [19]. For example, Minderest, a provider of price comparison software, markets its product as an "expert in price monitoring," showcasing how such software can facilitate competitive intelligence while raising concerns about its role in algorithmic collusion [76, 77].

Accurately defining and distinguishing algorithms is vital for identifying their role in collusion cases. For instance, in the Topkins and Eturas cases, pricing software provided to third-party users constituted distinct pricing algorithms. While the specifics of these algorithms differed between the two cases, each case also involved multiple algorithms within the same instance. The simultaneous use of multiple algorithms can significantly alter the structure and dynamics of collusion. Distinguishing between these algorithms requires detailed, case-specific analyses, where factors such as algorithm design, functionality, and intended purpose serve as key criteria for differentiation [15].

2.2. Algorithmic collusion formed by AI

Algorithmic collusion has been widely discussed by various scholars and institutions [15]. As early as in 2015, Mehra raised the question of "how antitrust will law work when decisions are no longer made by humans but instead by machines" [22]. Algorithm pricing and automatic decision making are considered to make cartel formation easier and more stable [22]. Mehra did not use the term "algorithmic collusion", but he has warned that algorithm pricing can contribute to collusion. In Ariel Ezrachi and Maurice E. Stucke's

"Virtual competition", they listed four types of "algorithmic collusion", including messengers, H&S, predictable agents, and digital eyes [13, 23]. However, Burden says that not all "algorithmic collusion" is genuinely algorithmic because they are simple tools to implement an existing instance of explicit collusion [15, 24]. Following terms offered in "Virtual competition", algorithmic collusions appeared in the working papers and reports in national competition authorities [15]:

Table 1. A comparison of terms of algorithmic collusion in the four doctrines

	The type of collusion and/or algorithm being used			
*Virtual Competition (*Ezrachi and Stucke)	Messenger	H&S	Predictable agent	Digital eye
Algorithms and Collusion (OECD)	Monitoring algorithms	Parallel algorithms	Signaling algorithms	Self-learning algorithms
Pricing Algorithms (UK CMA)	N/A	H&S	Predictable agent	Machine automation
Digital ecosystems, Big Data and Algorithms (Portuguese NCA)	Facilitating algorithms of explicit collusion and pre-existing vertical agreements	Common algorithms /H&S	Simple-rule pricing algorithms (predictable agent)	Self-learning algorithms
Algorithms and Competition (French and German NCAs)	Algorithms as supporters or facilitators of "traditional" anticompetitive practices	Algorithm-driven collusion between competitors involving a third party	Collusion induced by the (parallel) use of individual algorithms	

Source: Chen LI, Algorithmic Collusion and Artificial Intelligence: from the Perspective of EU Competition Law.

Among the four types of algorithmic collusion, digital eye is the closest form towards AI initiated algorithmic collusions because the algorithm has arrived at a high level of AI and is capable of learning from a large volume of data and updating itself [15]. OECD provides a definition to "collusion by a self-learning algorithm" as a "monopoly outcome even without competitors explicitly programming algorithms" [18]. To form an algorithmic collusion, the used algorithm should be one of machine or deep learning, a type of AI. These technologies are already "without explicit programming," [18] making them tantamount to the "digital eye" [15]. Japanese Fair Trade Commission discussed a more complicated algorithm, Q-learning, but it did exceed the definition provided by OECD. French and German competition authorities jointly issued a working paper to distinguish AI's initiation and implementation of collusion [25]. Collusions implemented by AIs are not truly algorithmic because they are initiated by human intervention. Such called "algorithmic collusion" has no differences from traditional one. Vestager's speech shows that it is possible to find the existence of truly AI-initated algorithmic collusion in the future, though collusion achieved without human intervention may be seen as science fiction at this point [26]. Even there are opinions that it already exists [27]. The algorithm in the digital eye or machine learning has achieved an AI level of super-human ability in

pricing and the exchange of relevant information. If AI can achieve collusion autonomously, it is likely to exist in a horizontal form of cartel [15].

Under EU compeition law, algorithm collusion is likely to fall in scope of Article 101(1) of TFEU. An agreement prohibited by Article 101(1) of TFEU therefore concerns a directly or indirectly fixed purchase price, selling price, or other trading condition. However, Article 101(1) of TFEU sets restrictive conditions on subject matters: agreement or concerted practice should be among competitors. Otherwise, this Article is not applicable. AI-initiated algorithmic collusion indeed brings challenges to Article 101(1) because the agreement may be "between some algorithms rather than undertakings" without human intervention [15]. This scenario will not involve any agreement between competitors, which diminishes the possibility of collusion. Concerted practice would be useful to identify algorithmic collusion, but it is still necessary to give a reason that a *de facto* agreement between AIs can be considered human coordination [15].

The situation would be different in China. Provisions on the prohibition of monopoly agreements (PPMA) by China's State Administration for Market Regulation (SAMR) provides norms on collusion facilitated by algorithms. Article 13 of PPMA rules that "business operators with competitive relations shall not use data and algorithms, technologies and platform rules to reach the monopoly agreement stipulated in Articles 8 to 12 through communication of intentions, exchange of sensitive information, and coordination of behaviour". Article 8(1) of PPMA provides the definition of relevant collusions: monopoly agreements on fixing or changing commodity prices, including (1) fixing or changing the price level, price changing range, profit level or other expenses such as discounts and handling fee; (2) agreeing to adopt standard formulas, algorithms, platform rules, etc. to calculate prices; (3) restricting the independent pricing right of operators participating in the agreement; (4) fixing or changing the price by other means [28].

In Chinese regulations, the identification on algorithmic collusion is much simplified. Not only simple agreement on using algorithm but also algorithm's faciliation on colllusion falls in the scope of Article 8 of PPMA. This simplificated norms on algorithmic collusion may result in a situation that collusion will be identified only if business operators use algorithm. However, Article 12 of PPMA use descriptions of "communication of intentions, exchange of sensitive information, and coordination of behavior", and requires the algorithmic collusion to be in an explicit form. If the collusion is explicit, it will be questionable whether it can be initiated by an autonomous AI. Chinese PPMA did not mention the use of AI, but straightly the rules on the use of algorithms. This means it is not important whether AI is autonomous or not. Besides horizontal collusion, PPMA also prohibits vertical agreements. Article 15 of PPMA rules that "business operators shall not use data and algorithms, technology and platform rules to reach the monopoly agreement stipulated in Article 14 of the cost provisions by unifying, limiting or automatically setting the price of resale goods" [28]. Article 14 of PPMA prohibits price fixing of resale price maintainence: (1) fixed price level, price change range, profit level or discount, handling fee and other expenses of resale goods to third parties; (2) limit the minimum price of resale of goods to third parties, or limit the minimum price of resale of goods to third parties through limited price change, profit level or other expenses such as discounts and handling

fees; (3) fix the price of resale goods or limit the lowest price of resale goods by other means [28].

2.3. Examples of algorithms in collusion

The OECD notes monitoring, parallel, signaling, and self-learning algorithms as their four concerns for competition, as shown in the table below [14].

Table 2. Summary of the roles of algorithms in implementing collusion

Role in implementing collusion	
Monitoring algorithms	Collecting and processing information from competitors and eventually penalizing deviations
Parallel algorithms	Coordinating parallel behavior, for instance, by programming prices to follow a leader, sharing pricing algorithms, or using the same third-party algorithm
Signaling algorithms	Disclosing and disseminating information to announce an intention to collude and negotiate a common policy
Self-learning algorithms	Maximizing profits while recognizing mutual interdependency and re-adapting behavior to the actions of other market players.

Source: OECD. (2017). Algorithms and collusion: Competition policy in the digital age. Also see Chen LI, Algorithmic Collusion and Artificial Intelligence: from the Perspective of EU Competition Law.

Two typical cases of so called "algorithmic collusion" are *U.S. v. David Topkins* in the U.S. and *Eturas* Case in the EU. In *Topkins* Case, The U.S. Department of Justice claimed that David Topkins and his conspirators used algorithms to fix the prices of posters sold on various online marketplaces including on the Amazon Marketplace [29]. David Topkins was found guilty because he had written the pricing algorithm for implementing the agreement and he was imposed a fine of 20,000 USD. The algorithm used in *Topkins* Case is not to initiate a colluision but to implement an already-existed human-initiated one. However, this algorithm has already been qualified as monitoring algorithm and the collusion is in the Messenger scenario as shown in Table 1.

In *Eturas* Case, the illegal behavior in the case was the sending by the online booking system Eturas of e-mails containing collusive information to users who were travel agencies on the platform [30]. The Eturas software is not autonomous, but it can automatically implement the price discount required by the platform. It is controversial whether Eturas platform's behavior is a unilateral conduct (not fall in the scope of Article 101(1) of TFEU) or a horizontal concerted practice, but European Court of Justice (ECJ) considers that the charged conduct is a collusion because the parties have obligations to refuse the price-fixing suggestion [15]. The algorithm in *Eturas* Case is a type of parallel algorithm listed in the table 2 and the collusion is H&S respectively. Both of two judicial cases do not refers to AI's initiation on algorithmic collusion, but they imply a possibility that AI's initiation of collusion may happen in the future.

3. Challenges posed by algorithmic collusion

3.1. Technical complexity

Li shows in its research a model of the internal structure of an algorithmic collusion initiated by two independent AIs in Figure 1. In this model, the collusion is initiated entirely between machines rather than a machine and a human operator. Compared with the situation in traditional collusion cases, the two independent AI do not need to interact with their users and designers when initiating algorithmic collusion.

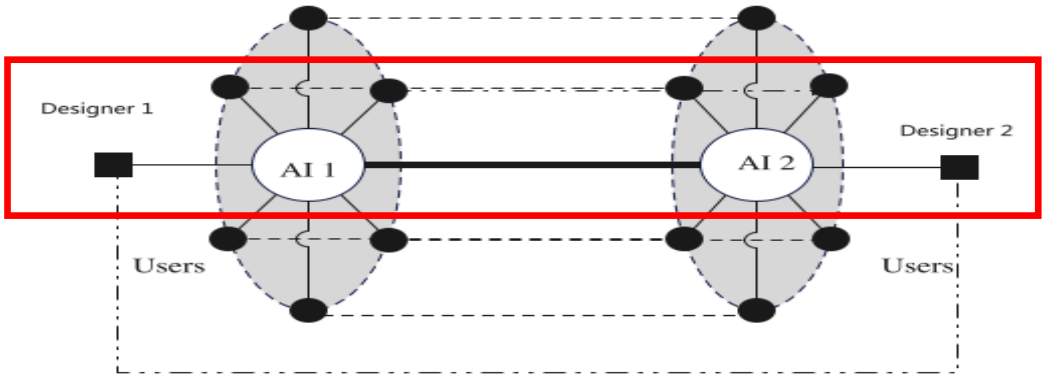

Fig. 1. The structure of algorithmic collusion initiated by two autonomous AI's conspiracy.
Source: Chen LI, Algorithmic Collusion and Artificial Intelligence: from the Perspective of EU Competition Law, University of Macau, 2023, p.138.

Even though the two AI are not human beings, they behave like two persons, and the communication between them looks like a kind of agreement of mankind [15]. The interaction between AIs is difficult to be detected by human operators, particularly for ordinary users. In this structure, eliminating effects on competition are established among algorithm users while the digital information exchange is between AIs. From the technological perspective, algorithm designers who provide such AIs are the most capable suject to detect the existence of the AI-initiated collusion. Therefore, the fact, the effect and the possible knowness of the algorithmic collusions separate into three different parties: AIs, users and designer. This raises questions on the location of the agreement and presents a challenge for liability [15]. Article 101(1) of TFEU only covers anticompetitive agreements and concerted practices between undertakings rather than AIs, so that it is difficult to ask for liabilities from algorithm users on such collusions.

3.2. Comparison with traditional collusion

As stipulated in the previous paragraphs, the key element in AI-initiated algorithmic collusion is that undertakings lack of direct communication as in traditional collusion. According to Li's thesis, this will challenge the traditional concept of agreement. *Bayer* case rules the essence of an agreement: "The existence of a concurrence of wills between at least two parties, the form in which it is manifested being unimportant so long as it constitutes the faithful expression of the parties' intention [31]".

There is no doubt that a concurrence of wills exists in traditional collusions as it was *Topkins* case. In traditional opinions, the agreement must be established between human operators rather than two non-human AI applications. In this digital scenario, the two parties can only be algorithm users according to traditional opinions [15].

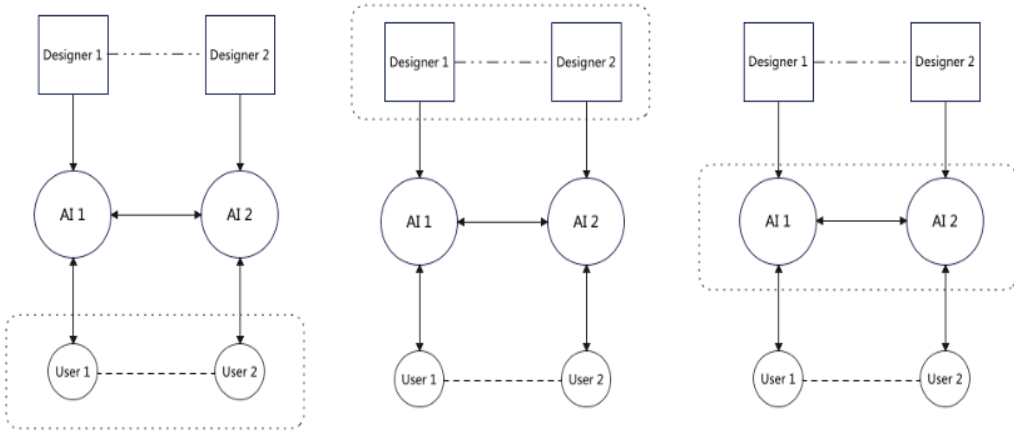

Fig. 2. Coordination between parties in algorithmic collusion initiated by two independent AIs.
Source: Chen LI, Algorithmic Collusion and Artificial Intelligence: from the Perspective of EU Competition Law, University of Macau, 2023, p.249.

Figure 2 shows three possible scenarios of coordination between two different parties, which either can be two users, two designers, or two AI applications. The coordination of the two independent AI applications is indeed a type of agreement-like behaviour, and the only difference is it is not between two persons. On one hand, the autonomy of two independent AIs should be respected because it is the basis of AI-initiated algorithmic collusions. Otherwise, AIs will not be important so that users will be totally liable. This is obviously unfair because the detection on AI's behavior is totally out of the capacities of ordinary users. This makes designer to escape from possible liabilities from creating a dangerous tool for the market competition. On the other hand, human operators should have a sufficient and necessary liability arrrangement because AI does not have any ability to bear liablity. AI cannot be an excuse for human operators to escape from initiation of algorithmic collusion as well as algorithm users (same role as parties in traditional collusions) should be attributed less liabilities than to the designers.

4. Solutions and proposals for improvement

AI-initiated algorithmic collusions make regulatory tasks more difficult. Current rules did not provide a proper approach for designers' liability. Even though David Topkins and Eturas are caught for being liable, current antitrust cases still do not provide sufficient norms on regulating the design of AI. David Topkins and Eturas companies manufactured relevant pricing algorithms, but those tools are not autonomous AI. Meanwhile, they also participated in collusion by themselves as parties. This means their liability is not absolutely caused by designing the software. Both U.S. and EU courts did not provide for immunity for the defendants in these two cases. This provides for the regulator to hold

algorithm designers liable, but it still needs a clear solution dealing with the autonomy of AI.

Chinese PPMA prohibits the use of algorithm to initiate collusion, and it can be a general rule to establish the illegality of algorithmic collusion. However, Chinese rules did not say anything on the behavior of designing a "guilty AI". Especially in scenarios when the pricing AI did not have functions for collusion at the moment when it is sold but gain relevant abilities during the process of learning in the real market environment by itself through analyzing data, there is no legal basis to require the designer to do supervision on the behaviors of AI in after sale market.

Both EU and China have rules on AI, for example Artificial Intelligence Act [32] (in the EU) and Interim measures for the management of generative AI services (in China) [28]. However, they are only for regulating AI collusion. Li's research clearly provides two reasons that pricing AI does not fall in the applicability of AI rules [15]. First, it does not have a physical body and cannot harm a natural person's health, security, or fundamental rights. Though some kinds of AI used in personal recommendations or ranking services can violate Article 102 TFEU and competition law, they do not appear in scenarios of algorithmic collusion. Secondly, pricing algorithms are used by undertakings for commercial purposes like price solutions rather than public policy. The subject matter influences how high-risk AI is identified. Though the same product is being used by two subjects, it is not regarded as high-risk unless the user is a public authority under Annex III. The European Union may add intelligent pricing algorithms into Annex II or expand the content of Annex III to include AI that harms competition in the scope of the Artificial Intelligence Act (the 2023 draft). Nevertheless, there is currently no channel for AI pricing algorithms to be regarded as high-risk.

There is still a long way for national competition authorities to find a solution to deal with the problem caused by AI. Regulations on AI provide promising approaches for imposing regulatory obligations on human operators. Intelligent pricing algorithms are already considered high-risk in competition law. The designer is expected to bear the most obligations in the prevention of collusion in both the design and after-sale stages. Efforts in the software manufacturing process may not prevent collusion, and the use of the AI must be supervised [15].

5. Balancing innovation and regulation

5.1. Regulation vs. innovation

Over-regulation can stifle innovation by imposing excessive constraints on researchers and developers. These constraints can limit creative freedom, slow down the pace of technological advancements, and increase the costs of innovation. Startups and smaller companies, in particular, may struggle to comply with stringent regulations, leading to reduced competition and a slower rate of progress in the AI industry [33]. Moreover, overly restrictive regulations can deter investment in AI research and development, as investors may perceive the risks and costs associated with compliance as outweighing the potential rewards [34].

In addition to financial and administrative burdens, over-regulation can also limit the scope of experimentation and risk-taking, which are essential components of innovation. For example, AI researchers might avoid pursuing groundbreaking but potentially controversial projects due to fear of regulatory repercussions [35]. This can lead to a more conservative approach to AI development, focusing on incremental improvements rather than transformative breakthroughs. Furthermore, stringent regulations can create barriers to entry for new players in the market. Established companies with more resources might be able to navigate complex regulatory landscapes, but startups and smaller enterprises may find it challenging to keep up [36]. This can reduce the diversity of ideas and approaches in the AI field, as innovation becomes concentrated in the hands of a few large entities.

Over-regulation may also slow the adoption of AI technologies across different sectors. Industries such as healthcare, transportation, and finance, which could benefit significantly from AI-driven solutions, might be hesitant to implement new technologies due to regulatory uncertainties [37]. This can delay the potential benefits of AI, such as improved efficiency, better decision-making, and enhanced user experiences. Moreover, strict regulations can lead to "regulatory capture", where well-established companies exert influence over the regulatory process, potentially leading to rules that favor them and hinder competition from smaller, innovative firms [38]. This phenomenon can exacerbate the concentration of market power and stifle innovation from newer entrants. However, it is important to recognize the need for a balanced regulatory approach that protects public interests without unduly hindering innovation. Effective regulation should aim to ensure safety, fairness, and accountability in AI applications while providing flexibility for innovation to thrive [39]. This can be achieved through adaptive regulatory frameworks that evolve with technological advancements, allowing for ongoing dialogue between regulators, industry stakeholders, and the public. Such a balanced approach can help mitigate the risks associated with AI, such as bias, privacy concerns, and ethical dilemmas, while fostering an environment where innovation can flourish. By finding the right equilibrium between regulation and innovation, society can harness the full potential of AI technologies to drive progress and improve quality of life [35].

5.2. Encouraging ethical AI in the smart economy

Promoting ethical AI development is essential to ensure that AI-driven technologies, including algorithmic pricing, operate fairly and transparently while aligning with societal values. Ethical AI emphasizes accountability, fairness, and transparency in algorithm design and deployment, which are critical to maintaining trust in the smart economy.

A key strategy to encourage ethical AI is the implementation of robust guidelines and regulatory frameworks. For instance, the European Union's "Ethics guidelines for trustworthy AI" highlight principles like explicability, accountability, and fairness as core elements of ethical AI development [40]. These guidelines provide a foundation for developers to build AI systems that prevent bias, ensure transparency, and respect user privacy.

Industry best practices also play a crucial role in fostering ethical AI. Collaborative initiatives, such as the "Partnership on AI", unite stakeholders across academia, industry, and civil society to develop shared ethical standards and promote the responsible use of AI

technologies [41]. Similarly, companies like Google have adopted internal AI ethics boards and issued principles to guide responsible AI development, addressing challenges such as algorithmic bias and the unintended consequences of autonomous systems [42].

Another practical step is investing in ethical AI research and training programs to equip developers with the skills to identify and mitigate ethical risks. By incorporating fairness metrics and bias-detection tools in the design phase, developers can create more equitable systems. For example, IBM's open-source tool "AI Fairness 360" enables developers to detect and address bias in their algorithms, setting a standard for transparency and fairness in AI models [43].

Finally, fostering an industry culture that values ethical practices can encourage compliance with these principles. Incentivizing adherence through certifications, such as those proposed by the "IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems**"**, ensures ethical considerations remain integral to AI development [44]. By integrating these strategies, the smart economy can leverage the benefits of AI-driven technologies while minimizing ethical concerns and safeguarding competition.

5.3. Role of self-regulation

Self-regulation plays a critical role in fostering ethical and competitive practices in the smart economy, complementing formal legal standards. While legal frameworks provide the foundation for addressing algorithmic collusion and ensuring fair competition, they often struggle to keep pace with rapid technological advancements. In this context, self-regulation emerges as a proactive and adaptive approach to fill the gaps between evolving technologies and existing laws.

The importance of self-regulation lies in its ability to address specific industry needs while promoting a culture of responsibility among stakeholders. Industry-led initiatives can establish codes of conduct, best practices, and technical standards tailored to the unique challenges of algorithmic pricing and AI deployment. For example, organizations like the "Partnership on AI" actively encourage companies to integrate ethical considerations into algorithm design and implementation, reducing the risk of unintended collusion [41].

Moreover, self-regulation fosters collaboration among businesses, academics, and policymakers, creating an ecosystem of shared accountability. By adopting voluntary compliance measures, companies can demonstrate their commitment to ethical practices and reduce the likelihood of regulatory intervention. For instance, self-imposed transparency requirements, such as auditing AI algorithms for anti-competitive risks, can enhance trust among consumers and regulators [2].

However, the effectiveness of self-regulation depends on widespread industry participation and robust enforcement mechanisms. Without these, voluntary measures risk being superficial or inconsistent. Therefore, self-regulation should operate alongside legal standards, with policymakers incentivizing adherence through recognition or integration into broader regulatory frameworks.

By combining the flexibility of self-regulation with the authority of legal standards, the smart economy can achieve a balanced approach that promotes innovation while safeguarding market fairness.

6. Conclusions

AI-initiated collusion introduces unprecedented complexities that traditional competition law frameworks struggle to address. Unlike human-initiated agreements, the interactions between autonomous AIs can mimic human-like agreements yet lack the direct involvement of human operators. This disconnect complicates the attribution of liability, as responsibility is fragmented across users, designers, and the autonomous systems themselves. Current legal frameworks, such as Article 101(1) of TFEU, are insufficient to handle these nuances, necessitating an evolution in how liability and agreements are defined.

A key distinction between traditional and AI-initiated collusion is the absence of direct human involvement in the latter. While traditional cases hinge on a "concurrence of wills" among human operators, AI systems establish agreement-like behaviors autonomously, challenging existing legal definitions. This shift demands new perspectives on liability, emphasizing the need for designers to bear a significant share of responsibility due to their role in creating and deploying potentially collusive AI systems. Existing regulatory frameworks, such as the EU's Artificial Intelligence Act and China's PPMA, inadequately address the unique risks posed by AI in pricing algorithms. While these rules govern high-risk AI applications, they fail to encompass autonomous pricing algorithms that indirectly harm market competition. Clear legal provisions are required to regulate AI design and ensure post-sale supervision of AI behaviors, particularly in cases where AI evolves through unsupervised learning.

Over-regulation risks stifling innovation, particularly for startups and smaller enterprises, by creating barriers to entry and limiting experimental freedom. Conversely, insufficient regulation can lead to ethical breaches, market distortions, and public distrust. A balanced approach is essential, one that combines adaptive regulatory frameworks with incentives for ethical AI practices. This balance can mitigate risks without curbing technological advancement.

Encouraging ethical AI practices in the smart economy is pivotal. Strategies such as robust regulatory guidelines, industry best practices, and investments in ethical AI research provide pathways for creating transparent, fair, and accountable AI systems. Collaborative efforts between regulators, industry, and academia can further ensure that AI technologies align with societal values while maintaining competitive markets.

To address the challenges of AI-initiated algorithmic collusion, regulatory innovation must evolve alongside technological advancements. By redefining liability frameworks, enhancing post-sale oversight, and fostering ethical AI development, policymakers and industry stakeholders can strike a delicate balance between promoting innovation and safeguarding market integrity. The successful integration of these approaches will ensure that AI technologies contribute positively to economic growth and societal progress.

References

[1] European Commission, "Shaping Europe's Digital Future," 2020.

[2] OECD, "AI in the Digital Economy: The Role of Innovation," 2021.

[3] C. Vrabie, "Promisiunile Inteligenței Artificiale (AI) administrației publice și orașelor inteligente," *Smart Cities International Conference Proceedings,* no. 11, 2024.

[4] I. Virtosu and C. Li, "Algorithms weighing lives and freedoms: The case of China's health code," *Smart Cities and Regional Development Journal,* vol. 7, no. 1, 2023.

[5] A. Labus and et al., "An IoT system for healthcare in the smart city," *Smart Cities and Regional Development Journal,* vol. 6, no. 2, 2022.

[6] K. Zela, "Exchange rate forecasting with Artificial Intelligence," *Smart Cities and Regional Development Journal,* vol. 7, no. 1, 2023.

[7] D. Ion, "Solving the traffic issue," *Smart Cities and Regional Development Journal,* vol. 1, no. 1, 2017.

[8] A. Iancu, "The importance of intelligent urbanism," *Smart Cities International Conference Proceedings,* vol. 8, 2023.

[9] X. Wen, "City intelligent life: A case study on Shenzhen city intelligent classification of domestic waste," *Smart Cities and Regional Development Journal,* vol. 5, no. 1, 2021.

[10] I. Virtosu and C. Li, "Vertical farming perspective and challenges: A comparative review between China and the EU," *Proceedings of the Central and Eastern European eDem and eGov Days, Association for Computing Machinery,* 2024.

[11] I. Virtosu and C. Li, "Smart life and sustainable development: a comparative analysis on energy and water efficiency in China and the EU," *Smart Cities and Regional Development Journal,* vol. 8, no. 5, 2024.

[12] M. Gal, "Algorithmic Challenges to Competition Law," 2020.

[13] A. Ezrachi and M. Stucke, "Virtual Competition: The promise and perils of the algorithm-driven Economy," 2016.

[14] OECD, "Algorithms and Collusion - Background Note by the Secretariat," [Online]. Available: https://one.oecd.org/document/DAF/COMP%282017%294/en/pdf.

[15] C. Li, Algorithmic collusion and Artificial Intelligence: from the perspective of EU competition law, PhD Thesis: University of Macau, 2023.

[16] B. Jang and et al., "Q-Learning algorithms: A comprehensive classification and applications," *IEEE Access,* vol. 7, 2019.

[17] C. &. M. A. Government of United Kingdom, "Pricing algorithms, Economic working paper on the use of algorithms to facilitate collusion and personalized pricing," 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_reporiskyrt.pdf.

[18] OECD, "Algorithms and collusion: Competition policy in the digital age," 2017. [Online]. Available: https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm.

[19] Competition Authority of Portugal, "Digital Ecosystems, big data and Algorithm," 2019. [Online]. Available: https://www.concorrencia.pt/sites/default/files/processos/epr/Digital%20Ecosystems%2C%20Big%20Data%20and%20Algorithms%20-%20Issues%20Paper.pdf.

[20] Minderest, "Price comparison software: Keys to choosing the Ideal Price Comparison Software," [Online]. Available: https://www.minderest.com/price-comparison-software.

[21] Minderest, "Price Intelligence & Competitor Monitor Software," [Online]. Available: https://www.minderest.com/?gclid=CjwKCAiA9JbwBRAAEiwAnWa4Q1z1LUvFUoO0NdqRAfOpX_rPSUh5HKbYpfRT55txjSwDzOgiesH-eBoCyzwQAvD_BwE.

[22] S. Mehra, "Antitrust and the Robo-Seller: Competition in the Time of Algorithms," *Minnesota Law Review,* 2016.

[23] Cyberspace Administration of China, "Interim Measures for the Management of Generative AI Services," 2023. [Online]. Available: https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm.

[24] K. Burden, "Computer Law & Security Review," 2017.

[25] Autorité de la concurrence & Bundeskartellamt, "Algorithms and competition," 2019. [Online]. Available: https://www.autoritedelaconcurrence.fr/sites/default/files/algorithms-and-competition.pdf..

[26] M. Vestager, "Algorithms and competition," *Bundeskartellamt 18th Conference on Competition,* 2017.

[27] A. Gautier and et al., "AI algorithms, Price Discrimination and Collusion: A technological, economic and legal perspective," *European Journal of Law and Economics,* vol. 50, no. 3, 2020.

[28] "Provisions on the Prohibition of Monopoly Agreements (PPMA) by China's State Administration for Market Regulation (SAMR)," 2023.

[29] "United States of America v. David Topkins. 3 15 CR 00201WHO, Information".

[30] "Eturas UAB et al v. Lietuvos Respublikos konkurencijos taryba, Case C-74/14, ECLI:EU:C:2016:42," 2016.

[31] "Bayer v. Commission, Case T-41/96, 4 C.M.L.R. 4. ECLI:EU:T:2000:242.," 2001.

[32] "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 an".

[33] World Economic Forum, "Reimagining regulation for the age of AI," 2020.

[34] M. Brundage and et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, 2018.

[35] L. Floridi, "Establishing the Rules for Building Trustworthy AI," *Nature Machine Intelligence,* vol. 1, no. 6, 2019.

[36] European Commission, "White Paper on Artificial Intelligence: A European approach to excellence and trust," 2020.

[37] S. Lohr, "AI Regulation is coming. Here's what to expect," *The New York Times,* 2020.

[38] M. Mitchell, Artificial Intelligence: A Guide for Thinking Humans, Farrar, Straus and Giroux, 2019.

[39] "Partnership on AI, Best Practices for Responsible AI," 2020.

[40] European Commission, "Ethics guidelines for trustworthy AI," 2019.

[41] "Partnership on AI, Collaborative efforts for ethical AI," 2020.

[42] S. Pichai, "Google's AI Principles: Responsible AI development," 2018. [Online]. Available: https://blog.google/technology/ai/ai-principles/.

[43] IBM, "AI Fairness 360: An open-source toolkit for detecting and mitigating bias in AI models," 2021. [Online]. Available: https://aif360.res.ibm.com/.

[44] I. G. I. o. E. o. A. a. I. Systems, "Ethical certification frameworks for AI systems," [Online]. Available: https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/.