Fair Competition in Digital Markets: Platform Power, Algorithmic Collusion, and the Arab Region's Next Steps

Sofiia Abdilatif, sofiaabdilatif@gmail.com
United Arab Emirates University, Al Ain, United Arab Emirates

Abstract

This paper examines challenges to fair competition in digital markets, focusing on platform gatekeeping, algorithmic complicity, and data-driven market manipulation. Looking through case studies from international and Arab markets, it evaluates regulatory responses by competition authorities in the EU, US, UK, ASEAN, and key Arab states including Kuwait, Saudi Arabia, and Egypt. The paper finds that where Arab regulators are increasingly active, there still are some gaps in ex ante gatekeeper rules, algorithmic auditing capacity, and cross-border enforcement. Practical, regionally grounded policy recommendations are proposed to protect consumers and competition in the Arab digital economy.

1. Introduction

Digital markets lower entry barriers for new businesses while simultaneously producing outcomes where a handful of platforms become nearly impossible to dislodge. Network effects, economies of scale, and data concentration combine to entrench dominant platforms, generating competition concerns the antitrust frameworks of the industrial age struggle (OECD, 2023).

This paper examines three competition problems: gatekeeping power,where dominant platforms control access to markets over dependent businesses; algorithmic collusion, by which pricing software coordinates prices across rivals without any human communication; and algorithmic market manipulation, most visible in cryptocurrency pump-and-dump schemes. The paper compares international and Arab regulatory responses and proposes some policy recommendations for the region's context.

2. Background

2.1. The Importance of Competition Law Enforcement in Digital Markets and its Impact on Markets and Consumers

The digital economy has transformed how goods, services, and information are distributed. According to UNCTAD (2021), digital platforms now mediate a growing share of global commerce, with the top five technology companies collectively controlling trillions of dollars in market capitalization. This concentration matters because dominant platforms shape what consumers can access, what prices they pay, and whether rival businesses can survive.

When competition fails in digital markets, the consequences extend beyond higher prices. Innovation slows as incumbents use data advantages and financial resources to acquire or foreclose potential rivals (Calvano et al., 2020). Consumer choice narrows as ecosystems close. Small and medium enterprises face asymmetric terms imposed by platforms on which they depend. The OECD (2024) has documented that 9 in 10 consumers have encountered manipulative design practices so-called "dark patterns" that distort purchasing decisions. Competition law enforcement is therefore not merely an economic regulatory

function; it directly affects consumer welfare, market access, and the basic fairness of the digital economy.

2.2. The Role of Competition Authorities in Enforcing Competition Law in Digital Markets: Definition, Objectives, Benefits, and Challenges

Public organisations known as competition authorities are in charge of monitoring mergers, encouraging market efficiency, and stopping anti-competitive behaviour. In digital markets, their role has expanded significantly. Traditional tools market definition, dominance analysis, abuse assessment, are still important but require adaptation. As de Streel (2022) explains, digital platforms create "bottleneck" intermediaries whose power cannot be assessed through conventional market share metrics; the focus must shift to their role as unavoidable intermediaries that third parties simply cannot bypass.

The main goals of competition enforcement in digital markets are to prevent anti-competitive foreclosure of rivals, make sure everyone has fair access to platform infrastructure, and maintain conditions in which innovation can flourish. Effective enforcement produces lower prices, greater consumer choice, and a level playing field for smaller businesses. However, digital markets bring big problems: they move faster than litigation timelines allow; algorithmic conduct leaves no paper trail of human coordination; and jurisdictional complexity means that a platform headquartered in one country can cause harm in another with limited legal exposure (International Competition Network, 2023). These structural challenges have driven a wave of regulatory innovation across multiple jurisdictions.

3. Case Studies

This section examines three areas of digital market competition concern gatekeeping power, algorithmic collusion, and algorithmic market manipulation each with dedicated analysis of the risk, followed by a case study drawn from international and, where relevant, Arab enforcement experience.

3.1. Risk 1: Gatekeeping Power

A gatekeeper, as defined by de Streel (2022), is an intermediary that controls access to a critical group of users in a way third parties cannot bypass. This bottleneck position allows the gatekeeper to unilaterally set rules for entire markets. Importantly, gatekeeper status is distinct from traditional market dominance: a company can qualify without holding a dominant position across every service it offers the focus is on its role as an unavoidable intermediary rather than its overall size (Grant Thornton, 2024).

Büchel and Rusche (2020) identify three structural enablers of gatekeeper power: vertical integration, which creates conflicts of interest between the platform and its business users; exclusive data access, which allows platforms to identify successful products among their sellers and launch competing versions with a notable informational head start; and the ability to shape consumer expectations such as next-day delivery standards in ways new entrants cannot feasibly meet. These advantages translate into specific anti-competitive practices, most prominently self-preferencing, which involves placing the platform's own products at the top of search rankings, and parity clauses that prevent sellers from offering better prices on competing channels.

Case Study: The EU Digital Markets Act and Gatekeeper Designation

The European Union's Digital Markets Act (DMA), in force since 2023, is the most comprehensive regulatory response to gatekeeper power globally. Rather than waiting for harm to occur and litigating after the fact, the DMA imposes binding obligations on the largest platforms before anti-competitive conduct takes place. A company is designated a gatekeeper if it exceeds €7.5 billion in annual EEA revenue or €75 billion in market capitalization, operates a core platform service with more than 45 million monthly EU users and 10,000 business users, and has held that position for at least three years (European Commission, 2023). As of 2024, seven companies Alphabet, Amazon, Apple, Booking.com, ByteDance, Meta, and Microsoft have been designated across 24 core services. Key obligations include:

- No "best price anywhere" requirements (Article 5(3)): platforms cannot force sellers to offer their lowest price through the platform, freeing them to compete on price elsewhere.
- No blocking direct customer contact (Article 5(4)): businesses may reach out directly to customers they found through the platform, without routing future contact through it.
- No using business users' data against them (Article 6(2)): gatekeepers cannot use confidential seller data to develop competing products.
- Fair and transparent rankings (Article 6(5)): gatekeepers cannot rig search results to favour their own offerings over rivals.
- Data portability (Article 6(10)): businesses have the right to access and export data their activity generates on the platform.

The Commission found that Apple's mandatory 30% commission, restrictions on alternative payment systems, and prohibition on developers directing users to lower-priced external channels constituted unfair trading conditions under the DMA (European Commission, 2024b). Apple is contesting the scope of these App Store obligations, arguing it operates five distinct stores across different devices rather than a single unified service. These disputes will determine how much practical force the DMA ultimately carries (Simone & Laudando, 2025).

In the Arab region, Egypt's Competition Authority (ECA) found that Apple and its distributors violated Egyptian Competition Law (ECA, 2026), representing one of the first major enforcement actions against a global technology company by an Arab competition authority. While the specific conduct has not been fully disclosed publicly, the case signals that Arab regulators are willing to act against dominant global platforms under existing national law, and that ex post enforcement is a viable near-term tool even without dedicated digital market legislation.

3.2. Risk 2: Algorithmic Collusion and Data Monopolies

Algorithmic collusion arises when competing firms use the same or similar pricing software, allowing algorithms to coordinate prices without any human communication. This constitutes a "hub-and-spoke" structure: the software provider acts as the hub, and the competing firms are the spokes (International Competition Network, 2023). Unlike traditional cartel conduct, there is no meeting, no phone call, and no explicit agreement yet the competitive effect is the same.

Research by Calvano et al. (2020) demonstrated that AI agents trained to maximize profits can independently learn to collude and penalize defectors without any explicit instruction to do so. Salcedo

(2024) extended this to large language models, showing that generative AI systems may drift toward collusive pricing depending on their training objectives. The OECD (2023) has also noted that firms with access to large, diverse datasets enjoy compounding competitive advantages, better data produces smarter algorithms, which produce stronger market positions, which in turn attract more data, making it very difficult for smaller players to compete. Combined with network effects, this dynamic can produce data monopolies that are extremely difficult for new entrants to contest (UNCTAD, 2021).

Case Study: European Commission Investigation into Algorithmic Pricing

In 2024, European competition authorities examined a pattern in which multiple online retailers used identical real-time price-matching algorithms. The mechanism appears competitive on its face: algorithms automatically match whichever competitor offers the lowest price. In practice, the effect is the opposite. When every retailer commits to matching the market's lowest price, no firm has any rational incentive to reduce prices, because any reduction would be immediately replicated by all competitors, eliminating the competitive gain that motivated the move. The result is a frozen market: prices stabilize at supra-competitive levels without any explicit agreement to keep them there. Economists call this a "price-matching equilibrium"; algorithmic implementation makes it enforceable at a scale and speed no human cartel could achieve (European Commission, 2024a).

The Commission concluded that these algorithms function as "tacit collusion enablers" and issued guidance clarifying that such outcomes may violate Article 101 of the Treaty on the Functioning of the European Union, the prohibition on anti-competitive agreements even in the absence of explicit human communication(European Commission, 2024a). This doctrinal shift is significant: it moves the legal test from intent to effect. The DMA reinforces this through Article 5, requiring gatekeepers to give advertisers and publishers access to performance measurement tools so they can independently verify whether algorithms treat them fairly.

Separately, the Commission used AI to analyze thousands of corporate earnings call transcripts, identifying two-word phrases statistically associated with price signaling among tyre manufacturers. An EU court accepted this AI-generated evidence as valid (COMMEO Rechtsanwälte, 2025). In the United States, the Federal Trade Commission opened a 2026 investigation into Instacart's use of an AI pricing tool called Eversight, which was found to charge consumers up to 23% more for identical items based on personal data, bringing algorithmic price discrimination into mainstream enforcement (Lexology, 2026).

In the Arab region, Kuwait's 2026 Guideline Manual for the consumer delivery services sector directly addresses practices that create or entrench algorithmic pricing advantages. Table 1 summarizes the prohibited practices and their competitive harms as defined by the Kuwait Competition Protection Agency.

Table 1: Kuwait CPA Guideline Prohibited Practices in Delivery Platform Markets

Practice	Definition	Competitive Harm
MFN Clauses	Forcing sellers not to offer better prices on competing platforms	Prevents inter-platform price competition

Self-Preferencing	Ranking the platform's own products above competitors'	Disadvantages third-party sellers
Exclusivity Requirements	Requiring sellers to deal only with one platform	Forecloses competitors from accessing sellers
Discriminatory Commissions	Applying different rates to similarly-situated sellers	Creates an uneven playing field
Predatory Pricing	Pricing below cost to eliminate competition	Reduces competition; prices rise post-exit

Source: Kuwait Competition Protection Agency (2026).

3.3. Risk 3: Market Manipulation Driven by Algorithms

Algorithmic market manipulation takes its most visible form in cryptocurrency markets, where the speed and pseudonymity of blockchain transactions create significant opportunities for abuse. As UNCTAD (2016) observed, the "invisible hand" that normally keeps markets honest is being replaced by a "digital hand" far more susceptible to manipulation. The classic pattern is the pump-and-dump scheme, which unfolds in three stages: an accumulation phase, in which organizers quietly acquire target tokens before any public announcement; a pump phase, in which coordinated social media campaigns across Telegram, Discord, and Twitter drive artificial price inflation within minutes; and a dump phase, in which organizers sell at the peak, leaving late-buying retail investors with losses. A 2025 study of over 1,000 tokens on the Poloniex exchange found that nearly 70% of pump events had a detectable prior accumulation phase, and that 24% of tokens launched in 2022 exhibited characteristics typical of pump-and-dump schemes (Bolz et al., 2025).

Regulators are responding with new detection tools. South Korea upgraded its VISTA trading analysis platform with AI capabilities designed to detect manipulation in real time (Yahoo Finance, 2026). Spain's CNMC established an Economic Intelligence Unit that automatically flags suspicious conduct (CNMC, 2026). The OECD (2024) has separately documented that 9 in 10 consumers have encountered dark patterns hidden fees, fake countdown timers, and manufactured urgency that manipulate online decision-making at scale, a form of algorithmic consumer harm that is equally corrosive to market integrity even where it falls short of outright fraud.

Case Study: The Gotbit/Vortex Cryptocurrency Manipulation Case (2026)

In March 2026, the U.S. The Department of Justice charged ten individuals from four companies Gotbit, Vortex, Antier, and Contrarian with running a large-scale cryptocurrency manipulation scheme (IRS Criminal Investigation, 2026). The companies presented themselves as legitimate market makers providing liquidity to support healthy trading. In reality, they used algorithms to conduct wash trading on a massive scale: buying and selling tokens among themselves to create the appearance of genuine market activity, then selling their positions to real investors who believed the market was authentic. This is an automated, high-speed version of the classic pump-and-dump fraud.

The case required extensive international coordination. Three defendants, including two CEOs, were arrested in Singapore and extradited to the United States in a process involving the U.S. FBI, IRS Criminal Investigation, the Singapore Police Force, and Singapore's Attorney General's Office (IRS

Criminal Investigation, 2026). Two defendants have pleaded guilty and received prison sentences; more than $1 million in cryptocurrency has been seized; and remaining defendants face up to 20 years in prison if convicted (MEXC News, 2026).

The case establishes three important precedents for digital markets enforcement. First, geographic borders provide no reliable protection; executives operating from Singapore were successfully prosecuted in the United States. Second, algorithmic execution does not insulate conduct from existing fraud law; statutes can reach automated manipulation even when no individual personally executed each trade. Third, meaningful cross-border cooperation between law enforcement is achievable when agencies coordinate early. For Arab regulators, who currently lack dedicated cryptocurrency enforcement frameworks, this case provides both a legal template and a cooperation model.

3.4. Comparative Analysis of Regulatory Responses

Table 2 summarizes the key features and limitations of major regulatory approaches to digital competition across jurisdictions. The EU provides the most complete template, but Arab states cannot simply import it wholesale. A more practical path combines Kuwait's sector-by-sector guideline approach, Saudi Arabia's expanded merger control, and Egypt's enforcement precedent, as well as building the regional cooperation infrastructure needed to address cross-border algorithmic risks.

Table 2: Comparative Overview of Digital Competition Regulatory Frameworks

Jurisdiction	Framework	Approach	Gatekeeper Rules	Algorithmic Collusion	Key Weakness
EU	Digital Markets Act (2023)	Ex ante	Yes binding obligations on 7 designated gatekeepers	Article 101 guidance; DMA Art. 5 transparency obligations	Static thresholds may become outdated
United States	Sherman & Clayton Acts	Ex post litigation	None case-by-case only	FTC Instacart investigation (2026); DOJ crypto cases	Slow; no structural remedy for entrenched power
United Kingdom	DMCC Act (2024–25)	Hybrid	Strategic Market Status designation by CMA	Retail sector focus; iterative conduct codes	Discretion creates legal uncertainty
ASEAN	Non-binding guidelines	Voluntary	None	Limited technical capacity	No binding cross-border enforcement
Arab Region	National laws; Kuwait CPA guideline (2026); ECA Apple action (2026)	Primarily ex post, emerging	None yet	No explicit algorithmic rules	Fragmented; limited algorithmic auditing capacity

Source: Author's compilation based on European Commission (2023, 2024); Kuwait CPA (2026); GAC (2025); ICN (2023).

4. Conclusion and Recommendations

The Arab region stands at a pivotal moment. Early enforcement actions, Kuwait's 2026 delivery platform guideline, Egypt's Apple case, Saudi Arabia's record merger filings in 2025 (GAC, 2025) demonstrate both willingness and growing institutional capacity to regulate digital markets. Yet big holes are still there: no ex ante gatekeeper designation system, limited algorithmic auditing infrastructure, and weak cross-border enforcement mechanisms for digital collusion. Without a coordinated, forward-looking framework, Arab economies risk replicating the platform dominance patterns of Western markets but with weaker safeguards in place. The following six recommendations are calibrated to current institutional resources and designed to be actionable and scalable.

Recommendation 1: Establish an Arab Digital Markets Network (ADMN). Modeled on the European Competition Network, this standing body would allow Arab competition authorities to share enforcement intelligence, coordinate simultaneous inspections, and develop joint gatekeeper identification guidelines adapted to Arab market conditions. The Arab Competition Forum, currently convened annually by ESCWA in partnership with UNCTAD and the OECD (ESCWA, 2024), provides a natural institutional foundation. The key step is formalizing this into a permanent secretariat. The principal obstacle is political coordination across authorities with varying resources and legal mandates.

Recommendation 2: Invest in Algorithmic Auditing Capacity. Each major Arab competition authority—Kuwait's CPA, Saudi Arabia's GAC, and Egypt's ECA should establish a dedicated Economic Intelligence Unit modeled on Spain's CNMC unit, equipped with AI-based tools capable of detecting price-matching algorithms and coordinated pricing patterns. Training programs for digital market economists and data scientists are an essential prerequisite; without this technical capacity, legal frameworks cannot be meaningfully enforced. Authorities should also adopt fast-track procedures empowering them to issue interim measures within ten working days of opening a case, given that digital market harm can become irreversible quickly.

Recommendation 3: Adopt a 'Hub-and-Spoke' Algorithm Rule. Arab competition law should explicitly address algorithmic collusion through a rebuttable presumption: where multiple competing firms use the same algorithmic pricing tool and prices move together, the software provider and users bear the burden of demonstrating that the outcome was not the result of coordination. Consistent with the European Commission's 2024 Article 101 guidance, this can be implemented through regulatory guidance rather than immediate legislative reform, significantly lowering the implementation barrier.

Recommendation 4: Regulate Cryptocurrency Market Makers. Following the Gotbit/Vortex case, Arab financial and competition authorities should jointly require registration and real-time reporting of algorithmic trading strategies by market makers, prohibit wash trading and coordinated pump-and-dump schemes, and develop cross-border asset freezing mechanisms through the Arab Competition Forum. These measures address an area of demonstrated harm where Arab markets currently have no dedicated protection.

Recommendation 5: Introduce Sectoral Data Sharing Schemes. In delivery, e-commerce, and ride-hailing markets, Arab regulators should consider establishing neutral data trustees that aggregate and anonymize market data to give new entrants a meaningful competitive base. This reduces incumbent data monopoly advantages without requiring full portability mandates. Implementation must comply with Arab data privacy frameworks, including the UAE's Personal Data Protection Law, though competitive access and privacy protection are not inherently incompatible goals.

Recommendation 6: Future-Proof for Generative AI and Emerging Platforms. As large language models are increasingly used for commercial pricing (Salcedo, 2024), Arab authorities should require firms to document training data and reward functions for AI pricing systems, and prohibit the use of competitor-sensitive data in model training without consent. A regional white paper identifying early competition concerns in metaverse environments where virtual goods, personal identity data, and real-economy transactions converge published by 2027, would allow Arab authorities to engage proactively rather than reactively.

Taken together, these recommendations do not require replicating the EU's DMA wholesale. They are calibrated to current Arab institutional capacity where creating a credible pathway toward more comprehensive regulation as that capacity develops. Ultimately, the goal is not to inhibit digital innovation but to ensure its benefits are distributed fairly among businesses of all sizes and among all consumers.

5. References

Bolz, N., Hofer, M., & Paolella, L. (2025). Sentiment, price, and volume driven detection of cryptocurrency market manipulation: Pump and dump. TechRxiv.

Büchel, J., & Rusche, C. (2020). Competition in the digital economy: An analysis of gatekeepers and regulations (IW-Policy Paper No. 26/2020). German Economic Institute. https://ideas.repec.org/p/zbw/iwkpps/262020.html

Calvano, E., Calzolari, G., Denicoló, V., & Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. American Economic Review, 110(10), 3267–3297. https://doi.org/10.1257/aer.20190623

COMMEO Rechtsanwälte. (2025, October 29). Public signaling and the use of AI by the EU Commission to detect infringements (Case T-188/24, Michelin v European Commission).

de Streel, A. (2022). Gatekeeper power in the digital economy: An emerging concept in EU law (OECD Competition Committee Note, DAF/COMP/WD(2022)57). OECD. https://one.oecd.org/document/DAF/COMP/WD(2022)57/en/pdf

Egyptian Competition Authority (ECA). (2026). Enforcement action against Apple and its distributors under Egyptian Competition Law [Case summary]. Cairo: ECA.

European Commission. (2023). Digital Markets Act: Commission designates six gatekeepers [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

European Commission. (2024a). Algorithmic pricing and tacit collusion in digital markets: Guidance on Article 101 TFEU [Staff working document]. Brussels: European Commission.

European Commission. (2024b). Digital Markets Act: Commission opens non-compliance proceedings against Apple [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689

ESCWA (United Nations Economic and Social Commission for Western Asia). (2024). Fifth Arab Competition Forum: Advocacy and regional cooperation [Meeting summary]. Beirut: ESCWA.

General Authority for Competition (GAC), Saudi Arabia. (2025). Annual report on competition enforcement and merger review. Riyadh: GAC.

Grant Thornton. (2024, October 22). Determining gatekeepers under the Digital Markets Act. https://www.grantthornton.ie/insights/factsheets/determining-gatekeepers-under-the-digital-markets-act/

International Competition Network (ICN). (2023). Algorithmic collusion: Key issues and policy responses. ICN Secretariat.

IRS Criminal Investigation. (2026, March 30). Ten foreign nationals charged in an international operation targeting cryptocurrency market manipulation [Press release]. U.S. Department of Justice.

Kuwait Competition Protection Agency (CPA). (2026). Guideline manual for the consumer delivery services sector via smart platforms and applications. Kuwait City: CPA.

Lexology. (2026). FTC investigation into Instacart algorithmic price discrimination. https://www.lexology.com

MEXC News. (2026, April). U.S. cracks down on alleged crypto market manipulation network spanning four firms. https://www.mexc.com/news

OECD. (2023). Algorithms and collusion: Competition policy in the digital age. OECD Publishing. https://www.oecd.org/competition/algorithms-collusion-competition-policy-digital-age.htm

OECD. (2024, October 8). Stronger consumer protections needed to address current and emerging harms consumers face online. OECD Publishing.

Salcedo, B. (2024). Pricing algorithms and tacit collusion [Working paper]. Department of Economics, Pennsylvania State University.

Simone, C., & Laudando, A. (2025). Principles and obligations of the Digital Markets Act in regulating the economic power of gatekeepers: Positive, negative or trade-off effects? Electronic Markets, 35(1). https://doi.org/10.1007/s12525-025-00788-6

Spanish National Commission on Markets and Competition (CNMC). (2026). Economic Intelligence Unit (UIE). https://www.cnmc.es

UNCTAD. (2016). Data protection regulations and international data flows: Implications for trade and development. United Nations.

UNCTAD. (2021). Digital economy report 2021: Cross-border data flows and development. United Nations. https://unctad.org/webflyer/digital-economy-report-2021

Yahoo Finance. (2026). South Korea’s Financial Supervisory Service upgrades VISTA platform with AI detection capabilities. https://finance.yahoo.com