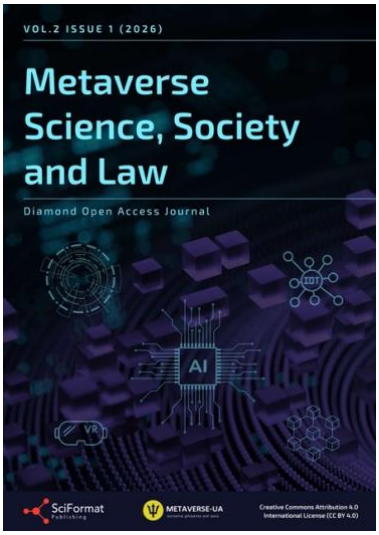


Metaverse Science, Society and Law

Vol. 2, Issue 1 (2026)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	ALGORITHMIC MECHANISMS OF UNFAIR COMPETITION IN DIGITAL MARKETS
DOI	https://doi.org/10.69635/mssl.2026.2.1.33
RECEIVED	11 December 2025
ACCEPTED	21 March 2026
PUBLISHED	30 March 2026
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

© The author(s) 2026.
This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

ALGORITHMIC MECHANISMS OF UNFAIR COMPETITION IN DIGITAL MARKETS

Gennadi Androshchuk
Candidate of Economic Sciences, Associate Professor, ChiefResearcher at the Research Instituteof Intellectual Property of the National Academy of Sciences of Ukraine
ORCID ID: 0000-0003-0781-9740

Vladislav Khvostenko
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity, National Technical University Kharkiv Polytechnic Institute, Ukraine
ORCID ID: 0000-0002-6436-4159

ABSTRACT

The article examines the transformation of unfair competition under conditions of digitalization and the growing dominance of platform-based business models. It argues that traditional anti-competitive practices increasingly acquire an algorithmic nature and are implemented through ranking systems, recommendation mechanisms, automated pricing tools, and large-scale data processing. The study identifies key algorithmic mechanisms of competitive distortion, including self-preferencing, visibility manipulation, algorithmic coordination, data opacity, interoperability restrictions, and the reinforcement of market power through network effects. It demonstrates that the interaction between data, algorithms, and platform infrastructure produces a new configuration of digital market power that challenges conventional competition law doctrines.

The paper develops an integrated economic and legal model of regulatory response that combines ex post antitrust enforcement with ex ante preventive obligations. The proposed model includes algorithmic risk detection, legal qualification of conduct, proportional remedial measures (transparency requirements, algorithmic audits, interoperability duties), and compliance monitoring. Particular attention is paid to the evidentiary challenges associated with algorithmic opacity and the need for adapted standards of digital proof. The scientific novelty of the research lies in the conceptualization of a systemic framework linking algorithmic mechanisms, digital market structures, regulatory instruments, and digital evidence in the context of contemporary antitrust control.

KEYWORDS

Digital Markets, Unfair Competition, Algorithmic Market Power, Digital Platforms, Competition Law, Ex Ante Regulation, Algorithmic Audit, Network Effects, Platform Governance, Regulatory Model

CITATION

Gennadi Androshchuk, Vladislav Khvostenko. (2026) Algorithmic Mechanisms of Unfair Competition in Digital Markets. *Metaverse Science, Society and Law*. Vol. 2, Issue 1. doi: 10.69635/mssl.2026.2.1.33

COPYRIGHT

© The author(s) 2026. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

Introduction.

The Paris Convention for the Protection of Industrial Property (Paris Convention) in Article 10-bis (2) defines that an act of unfair competition is any act of competition that is contrary to honest practices in industrial and commercial matters.[1] The WIPO Model Provisions on Protection Against Unfair Competition clarify the definition of 'unfair competition' contained in the Paris Convention, which *does does not refer to competitive relationships as one of the main criteria of this concept.*[2]

Many countries have already adapted these recommendations into their national legislation.

Unfair competition in digital markets covers a wide range of practices that aim to mislead consumers and distort competitive conditions, ultimately undermining consumer confidence and brand integrity. Such actions can manifest themselves through misleading advertising, data manipulation and intellectual property rights violations. These practices not only harm fair-minded businesses but also create market imbalances that can lead to reduced innovation and higher prices for end consumers. Digital platforms, with their ability to enable instant and large-scale interaction between millions of users, create unique benefits such as lower transaction costs, reduced information search costs, and efficient organisation of large amounts of data. They provide a huge number of potential counterparties for transactions or information exchange in a single environment, often at little or no cost to the end user. However, this same efficiency and ability to collect data on a massive scale create new challenges for competition.

The collection and use of user data allow platforms to strengthen their power over many aspects of the relationship between businesses and consumers. This consolidation of power creates conditions for unfair competition, as dominant players can use their position to gain unfair advantages, which in turn reduces incentives for innovation and potentially increases prices for consumers. Thus, the inherent efficiency of platforms, which contributes to their rapid growth and acquisition of market power through the accumulation and use of data, can become a source of unfair competition and anti-competitive practices.

Analysis of recent research and publications. The issues of competition law and protection against unfair competition have been studied by such domestic scholars (lawyers and economists) as Androshchuk G.O., Bakalinska O.O., Bezug O.V., Borysenko Z.M., Butnik-Siversky O.B., Valitov S.S., Voznyuk O.V., Dakhno I.I., ZhurykYu.V., Kapitsa Yu.M., Kodynec A.O. Lagutin V.D., Polyukhovich V.I., Smirnova K.V., Chernevska O.L., Shklyar S.V. and others. O.M. Vinnik made a significant contribution to the development of scientific and legal research on the digital economy, investigating specific issues of antitrust regulation in the digital economy.[3] However, the dynamic nature of changes in the economy and legislation in the field of the digital economy requires further scientific research.

The purpose of this article is to provide a theoretical justification for the transformation of unfair competition in the context of an algorithmic digital economy, to systematise the forms of algorithmic distortions of the competitive environment, and to develop a multi-level economic and legal model of regulatory countermeasures aimed at ensuring a balance between innovative development, market competition and consumer protection.

1. Transformation of Unfair Competition in Digital Markets

The enforcement of competition law is constantly evolving, adapting to the new realities of the digital economy. Antitrust authorities around the world are improving tools and methodologies to combat anti-competitive practices in various sectors of the economy. Particular attention is paid to the role of data in the provision of services by digital platforms, which attracts the close attention of consumers, businesses and regulators.

The European Union (EU) has become one of the leaders in developing new regulations by introducing the Digital Markets Act (DMA), which came into force on 7 March 2024[4]. The DMA is a central element of the European digital strategy, designed to regulate large online platforms, the so-called 'gatekeepers'. This law represents a fundamental change in the approach to regulation. Traditional antitrust legislation often responds

[1]Bodenhausen G. Paris Convention for the Protection of Industrial Property: Commentary / trans. from English, prefaced and scientific ed. by G.O. Androschuk. Kyiv: Parliamentary Publishing House, 2018. - 264 p.

[2]Androschuk G.O. Competition law: protection against unfair competition../ G.O. Androschuk, S.V. Shklyar - Scientific and practical edition. – K.: Justinian, 2012. – 472 p.

[3]Vinnyk O. M. The Law of the Digital Economy. Kyiv: Research Institute of Private Law and Entrepreneurship named after Academician F. H. Burchak of the National Academy of Law Sciences of Ukraine, 2021. 350p. Repository of Academic Texts of Academician F. H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of the National Academy of Law Sciences of Ukraine. URL: https://t.ly/osxVj.

[4]The Digital Markets Act URL:https://digital-markets-act.ec.europa.eu/index_en

to violations *after* they have occurred (ex post). However, the rapid development and unique characteristics of digital markets, such as network effects, data accumulation and 'winner-takes-all' dynamics, make such interventions less effective or too slow. The DMA's approach, based on ex ante regulation, aims to prevent abuse by setting clear 'dos' and 'don'ts' for gatekeepers before the damage is fully realised. This reflects the recognition that the speed and scale of the digital market's evolution require a more proactive regulatory stance to maintain competitiveness and stimulate innovation.

In his study, V.I. Polyukhovichnotes:"Digital markets are electronic platforms that operate on the basis of digital technologies on the Internet, are sources of information and allow electronic transactions to be carried out on the basis of this information, which serve as the basis for the movement, exchange, purchase and sale of goods, works and services. They bring together sellers and buyers in a virtual environment and include a wide range of economic interactions — from e-commerce and financial transactions to various online services. Digital markets have such characteristics as global access, high speed of information exchange, low transaction costs, and the availability of large amounts of data that influence market competition, consumer choice, and shape supply[1].

The digital market in the field of intellectual property is a set of social relations arising in the digital environment regarding the creation, acquisition, exercise, transfer, licensing and protection of property and non-property rights to intellectual property objects. It operates through digital platforms, electronic services and algorithmic systems, which act as infrastructure elements for the enforcement and application of rights.

The specificity of such a market lies in the transnational nature of legal relations, the absence of a physical link between the object and the territory of a particular state, and the simultaneous application of the norms of different jurisdictions. This leads to the increased importance of conflict of laws regulation, international harmonisation of legislation and the development of supranational coordination mechanisms. The digital environment is significantly transforming the traditional institutions of copyright, patent law and trademark law, as objects are circulated in the form of electronic reproduction, public disclosure, digital distribution and remote licensing.

At the same time, the digital nature of the market creates a complex set of new legal risks. In particular, it significantly simplifies the possibility of unauthorised copying and distribution of IP objects, and creates difficulties in identifying the offender, proving the fact of the infringement and determining the competent jurisdiction. Additional challenges include online fraud, phishing schemes, the unlawful use of trademarks in digital advertising, algorithmic underestimation of the visibility of the rights holder, and the unfair use of data on IP objects.

In response to these challenges, comprehensive regulatory approaches are being developed in legal systems to ensure a balance between the freedom of digital information circulation and the effective protection of intellectual property rights. An example is the European Union's Digital Single Market initiative, which provides for the harmonisation of rules on access to digital content, the strengthening of platform accountability mechanisms, and the unification of standards for the protection of consumers and rights holders.

Thus, the digital market in the field of intellectual property should be viewed not only as an economic system for the circulation of intangible assets, but as a complex, multi-level legal construct that combines the norms of private and public law, national and international regulation, and self-regulation mechanisms for digital platforms.

Digital platforms for IP: These are technological solutions and online services that facilitate the management, licensing, protection and commercialisation of IP. **Main functions and types of platforms: Platforms for content distribution and licensing:** Streaming services (music, video) Online stores for software and e-books. Marketplaces where authors can sell their works (e.g., photo stocks, platforms for 3D models). **Platforms for IP management and protection:** Blockchain-platforms **(**e.g.**,** Story **(**IP**))**: Used to reliably and immutably record information about authorship, creation time, transactions, and licensing of IP objects. This helps automate the rights management process and protect against counterfeiting. Digital Rights Management (DRM) systems: Technologies for controlling the use of digital content. Platforms for patenting and trademarks: Online services of national and international agencies that simplify the submission of applications and management of IP portfolios. **Collaboration and innovation platforms:** Tools for team development and project management that record each participant's contribution (e.g., *Notion* and *ClickUp* can be used indirectly to record the creation process). **Impact on the IP sector:** The digital market and platforms

[1]Valeriy Polyukhovich Protection of economic competition in digital markets in Ukraine // University Scientific Notes, – Khmelnytskyi. 2024. No. 5 (101), pp. 17-30. DOI 10.37491/UNZ.101.2

create new opportunities, but also challenges: **Monetisation:** New models such as subscriptions, micropayments and asset tokenisation (NFT). **Accessibility:** Simplifying access to IP for consumers and simplifying procedures for rights holders. **Protection:** Increased need for digital protection mechanisms (DRM, blockchain) and updating legislation to combat online piracy.

Given the transnational nature of the digital market in the field of intellectual property, the multi-level structure of legal relations and the algorithmic mediation of economic interaction, there is a need to systematise its institutional and technological components. The digital IP market cannot be viewed solely as a collection of economic entities or as an e-commerce tool; it functions as a complex multi-layered system that combines legal regulatory mechanisms, institutional architecture, platform-based access organisation, algorithmic data processing and technical infrastructure.

To fully reflect this structure, it is advisable to use a multi-level model that allows visualising the interaction of participants in the digital IP market and tracing the links between the legal, institutional, platform, algorithmic and technological levels of its functioning.

The corresponding model is presented in Fig. 1.

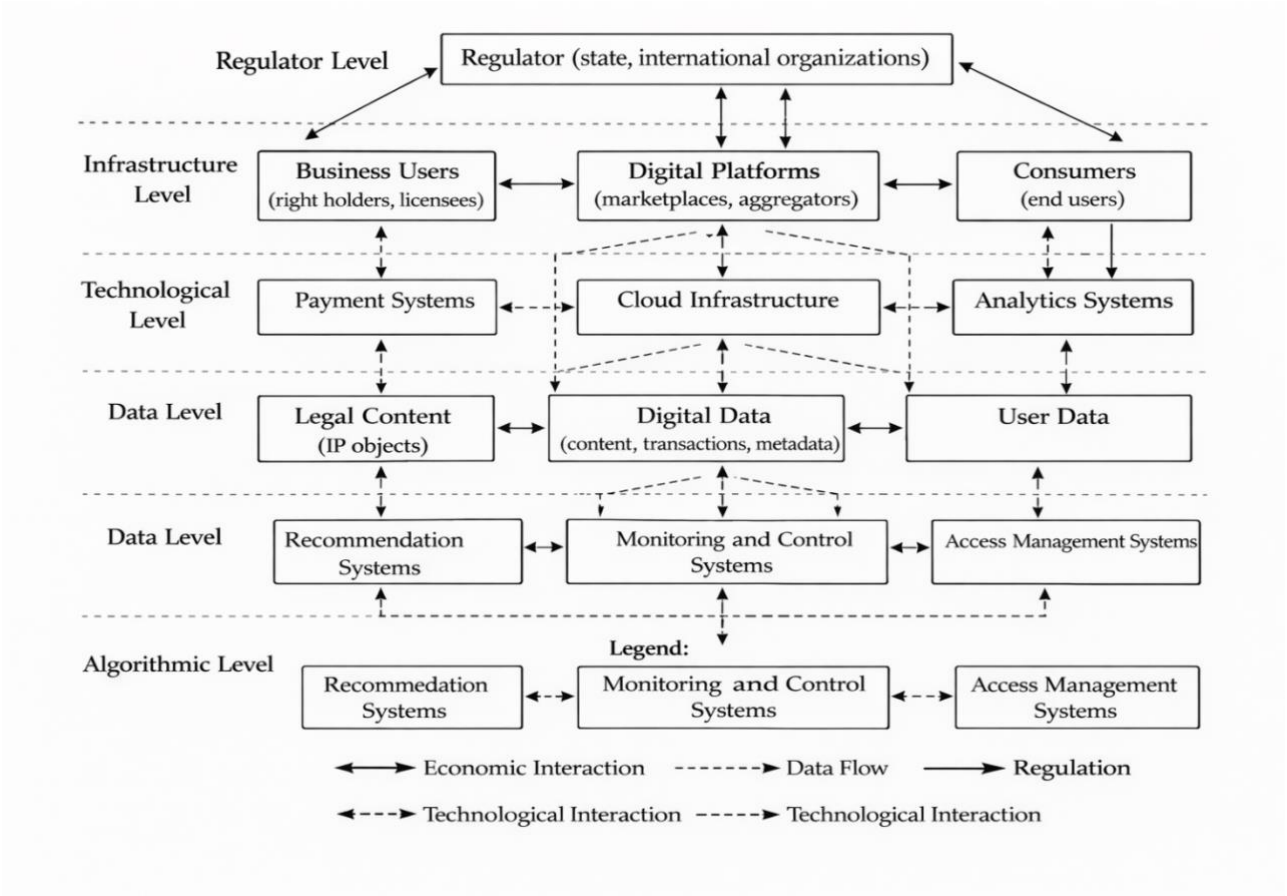


Fig. 1. *Diagram of network interaction between participants in the digital intellectual property market*

The proposed multi-layered model demonstrates that the digital intellectual property market is a system of interconnected levels within which the economic and legal interaction of entities is formed and implemented. Digital platforms occupy a central place in this system, providing access to IP objects, accumulating and processing data, and mediating relations between rights holders and consumers.

2. Algorithmic Mechanisms of Market Distortion and Competitive Manipulation

The algorithmic and information levels perform the function of redistributing economic value, while the legal and institutional levels form the normative boundaries of acceptable behaviour. The technical infrastructure, in turn, provides the material and technological basis for the functioning of the entire system.

Thus, the digital IP market should be viewed as an integrated, multi-level ecosystem in which market power concentration, algorithmic mediation, and regulatory mechanisms are in constant interaction. It is this structural complexity that creates the preconditions for both innovative development and the emergence of risks of unfair competition, which requires further systematic analysis.

Significance for consumers and innovation. Unfair competition also occurs in digital markets, which can take the form of spreading false information about competitors' goods, services or business reputation, illegal use of trademarks, industrial designs (designs) or other industrial property of competitors, as well as in the disclosure or use of a competitor's trade secrets without their consent. [5, pp. 26-27] Unfair competition in digital markets has negative consequences for consumers and innovation. It distorts market dynamics, which can lead to a decline in innovation, as firms lose incentives to develop new products if competitors can engage in unfair practices. In addition, it can lead to higher prices for consumers due to a lack of competition, which reduces their purchasing power. Another important consequence is the undermining of consumer trust, as users become wary of manipulative practices.

The Digital Markets Act (DMA) aims to ensure fair competition, prevent abuse of power and market position, and protect consumer privacy online. It aims to give consumers more choice, better services and fairer prices, as well as ensuring direct access to services.

The erosion of consumer trust caused by unfair practices is not just a consequence, but also a mechanism that exacerbates market distortions. When consumers lose trust in online information due to misleading advertising or fake reviews, they become more risk-averse. This can lead them to stick with established, dominant platforms or brands that they *perceive* as reliable, even if those platforms may engage in self-preferencing. This reluctance to explore alternatives, fuelled by mistrust, further strengthens the market power of dominant players, making it difficult for new, innovative market entrants to gain a foothold. As a result, it stifles overall innovation in the market. Thus, unfair practices lead to a decline in consumer trust, which in turn reduces their willingness to switch suppliers, entrenches dominant players and, as a result, slows down innovation.

Search engine manipulation (SEO spam, keyword stuffing).

Definition and types of SEO spam.SEO spam, also known as spamdexing, is a set of unethical methods used to manipulate the ranking of web pages in search engine results. These tactics, often classified as ‘black hat’ SEO methods, may bring short-term benefits, but in the long run, they seriously damage trust in the website, lead to penalties from search engines, and even complete removal from search results (SERP).[1]

One of the most common forms of SEO spam is **keyword stuffing**. This is an unethical practice that involves overfilling a web page with target keywords in order to manipulate rankings. Search engines easily detect such actions and apply sanctions, as content oversaturated with keywords is often unreadable and useless to users.

Keyword stuffing can be implemented in two main ways:

Visible stuffing: This occurs when keywords are repeated excessively and unnaturally in the text, being visible to the reader, often out of context. An example would be: "Looking for the best vacuum cleaner? You've come to the right place for the best vacuum cleaner. Our brand offers the best vacuum cleaner you could ever want. Lightweight yet powerful, it is the best vacuum cleaner for all your cleaning needs. The best vacuum cleaner." This use of terms is excessive and irrelevant. It can also include the unnatural addition of a long list of keywords in a paragraph.

Invisible content: This method involves hiding spam text from readers but leaving it accessible to search engine robots.

This can be achieved by using text that is the same colour as the page background or by placing keywords in invisible parts of the web page, such as image alt text, meta tags or comments in the HTML code.

In addition to keyword stuffing, there are other common forms of SEO spam[2]:

[1]Sanja TrajchevaWhat is SEO Spam and How Does It Impact Your Site?URL:What is SEO Spam and How Does It Impact Your Site?
[2]Aaron R. Winston 10 SEO Spam Types & How to Avoid: Personal Injury Lawyers URL610 SEO Spam Types & How to Avoid: Personal Injury Lawyers

Buying Backlinks: This involves creating artificial links to a website from other resources, often from irrelevant or spammy sources, in order to manipulate the page's authority (‘link juice’).

Duplicate Content: Placing identical or nearly identical content on multiple pages confuses search engines, as it is difficult for them to determine the most relevant version, and can negatively affect rankings.

Low-Quality Content: Creating content that does not provide value to users and is only intended to manipulate rankings.

Hidden Text and Links: Placing text or links that are not visible to users but are accessible to search engines.

Clickbait Titles and Meta Descriptions: Using misleading titles and descriptions to attract clicks.

Comment Spam: Posting irrelevant comments with links to other websites, blogs, or forums.

Doorway Pages: Creating pages that automatically redirect users to another resource without providing relevant content.

Cloaking: A practice in which the information presented to a search engine differs from that displayed to users. For example, a page may be about hotel reservations, but content about pharmaceutical products is presented to the search engine.

Japanese Keyword Hack: An unusual but common SEO spam technique that involves injecting Japanese characters and content into a website, usually by brute force, to generate backlinks to fraudulent resources.

Impact on search results, user experience and market integrity. Search engine manipulation has a negative impact on search results, user experience and market integrity.

Negative impact on SEO: Search engines such as Google and Bing clearly state that keyword stuffing violates their guidelines. They actively downgrade or remove sites that engage in such practices. Modern search engines are very sophisticated: updates such as Hummingbird, BERT, and MUM have allowed Google to better understand context, synonyms, and user intent, rather than just the number of keyword occurrences. This means that manipulative tactics are ineffective, and Google uses manual actions or automated systems to detect and penalise such content.

Deterioration of user experience: Content that is oversaturated with keywords is often unreadable and unhelpful to users. This leads to a high bounce rate, which in turn signals to search engines that the page is of low quality, resulting in a lower ranking. Search engines favour pages that provide an excellent user experience.

Distortion of search results: Manipulation of search engines distorts results, making it difficult for users to find relevant and quality information. This has far-reaching consequences, influencing consumer decisions. For example, an experiment showed that manipulating search results can change voters' opinions, with the probability of influencing voting reaching 25% for the most susceptible groups of the population. It is difficult for end users to detect such manipulation because they interact with the search engine a limited number of times and do not have the expertise to detect bias.

The evolution of SEO spam is an ongoing battle between manipulators and search engines, where complex algorithms driven by artificial intelligence (AI) adapt to detect and penalise ‘black hat’ tactics. Initially, simple keyword stuffing could be effective, but search engines quickly learned to detect it. This prompted spammers to use more covert methods, such as cloaking or hidden text. In response, search engines developed more sophisticated algorithms that understand context and user intent, rather than just keyword density. This continuous adaptation shows that what was once effective is now detrimental, as penalties are severe. This shifts the competitive landscape from technical manipulation to creating real value, requiring effective SEO to focus on user experience and high-quality, natural content. It should be noted that the defence of search engines such as Google against accusations of unfair competition, particularly in prioritising their own services, is often based on the argument that their search results are a form of ‘speech’ protected by the First Amendment (to the US Constitution, which proclaims the general freedoms of citizens). If search results are indeed classified as speech, then regulating their ranking to prevent self-preferencing or other forms of manipulation becomes constitutionally problematic. This creates tension between the principles of free speech and antitrust goals, potentially allowing dominant platforms to justify practices that distort competition under the guise of editorial freedom. This highlights a significant legal challenge in applying traditional antitrust frameworks to new digital market structures. Given the multi-layered nature of the digital IP market, algorithmic mechanisms can be used not only as a tool for search optimisation and personalisation, but also as a means of distorting the competitive environment. In order to systematise relevant practices, a classification of forms of algorithmic manipulation by infrastructure level and nature of competitive effect is proposed. This is shown in Table 1.

Classification of forms of algorithmic manipulation

Class of manipulation	Specific form	Level of infrastructure	Mechanism of influence	Competitive effect	Legal classification
I. Ranking manipulation	Key word stuffing	Algorithmic	Artificial boosting of relevance	Visibility distortion; competitor displacement	Unfair competition
	Hidden text	Algorithmic	Deceptive algorithm input	Violation of equal access	Misleading practices
	Cloaking	Platform–algorithmic	Presenting different content to algorithm and user	Indexing distortion	Unfair competition
II. Behavioural signal manipulation	Comment spam	Data level	Artificial popularity creation	Loss of market trust	Unfair practice
	Fake reviews	Data level	Imitation of social proof	Information asymmetry	Consumer deception
	Bot traffic	Technological	Artificial formation of behavioural metrics	Manipulation of algorithmic promotion	Unfair competition
III. Content manipulation	Door way pages	Algorithmic	Traffic redirection	Audience capture	Unfair competition
	Content duplication	Data level	Copying digital object	Copyright infringement	IP violation
IV. Algorithmic discrimination	Self-preferencing	Platform	Prioritisation of own content	Restriction of competition	Abuse of dominance
	Algorithmic collusion	Algorithmic	Coordinated pricing via AI	Market distortion	Anti-competitive agreement

An analysis of the forms listed above shows that algorithmic manipulation is a multi-level phenomenon that encompasses both direct interference in ranking mechanisms and indirect distortion of behavioural signals and the information environment. The most dangerous practices from the point of view of market stability are those that combine algorithmic advantage with platform access control, as they are capable of creating persistent barriers to entry and concentrating market power.

Use of bots to manipulate reviews and ratings. Definition and methods of manipulation using bots.

Fake reviews are deliberately misleading ratings or reviews that distort the truth about a business or product. They can come from a variety of sources, including sellers, third-party agencies, automated bots, or competitors, making them increasingly difficult to detect.

Methods of manipulation using bots and fake reviews include:

Artificially inflating popularity: Fake 5-star reviews are used to artificially inflate the perceived quality of a product or service. For example, it is extremely rare to find a product on Amazon with only 5-star reviews, and such a pattern may indicate fraudulent activity.

Damaging competitors' reputations: Fake negative reviews damage a brand's reputation and mislead consumers. This may be a coordinated attack by a competitor.

Manipulation of consumer behaviour: Content generated by bots is not a genuine human experience, which distorts engagement metrics and influences purchasing decisions. Fake reviews can stimulate the desire to buy by changing perceptions of demand or influencing the evaluation of alternative plans.

'Network water army': These are groups that operate with a high level of concealment and group operations, creating fake and malicious marketing.

Brushing: The practice of manipulating reviews to mislead the public about a store's actual performance, influencing consumer behaviour.

Misleading incentives: Some consumers write fake reviews in exchange for free products, discounts, or other bonuses offered by brands. An example is the case of skincare brand Sunday Riley, which instructed its employees to write fake positive reviews on the Sephora website.

Impact on consumer trust, purchasing decisions and fair competition. The impact of fake reviews and bots on consumer trust, purchasing decisions, and fair competition is significant and devastating.

Erosion of consumer trust: Fake reviews and boots pose a serious threat to consumer trust and brand reputation. According to BrightLocal's 2023 report, 98% of consumers read online reviews, and unfortunately,

42% of them have encountered what they believe to be fake reviews[1]. The use of bots to artificially generate content on a large scale further undermines consumer trust in brands, which may be perceived as deceptive or manipulative. Even genuine and authentic reviews may be met with increasing scepticism due to the prevalence of fake ones.

Distortion of purchasing decisions: Fake reviews create significant obstacles for consumers in making the right purchasing decisions. They can stimulate the desire to buy by changing perceptions of demand or influence the evaluation of alternative plans. In the era of big data and information technology, faced with numerous sellers and limited time, consumers typically focus on the seller's trustworthiness and other consumers' ratings when choosing products. The practice of 'brushing' can mislead the public about the actual performance of a store, which ultimately influences consumer purchasing behaviour.

Unfair competition: Fake reviews create unfair competition in the market. Less competitive companies often use them as a quick way to artificially improve their image, while higher-quality competitors may suffer from targeted negative reviews. This manipulation undermines the fairness of the e-commerce ecosystem, which should reward businesses based on their authentic reputation.

Social and political risks: Beyond their impact on brand reputation, bots can have significant social and political implications. A 2019 study found that social bots played a 'disproportionate role in spreading misinformation online' during the 2016 US presidential election, with 6% of Twitter accounts identified as bots spreading 31% of low-trust information.

The advent of generative artificial intelligence (AI) has significantly complicated the problem of fake reviews, turning their detection from simple pattern recognition into complex linguistic and behavioural analysis. While fake reviews have always been a problem, the advent of generative AI means that they are becoming 'more sophisticated and difficult to detect.' This marks a shift from simple, easily identifiable patterns (e.g., generic language, sudden spikes) to more complex, human-like content. Therefore, detection methods must evolve from basic pattern analysis to advanced AI-based linguistic analysis. This escalation of competition between AI-generated fraud and AI-driven detection places a greater burden on platforms and regulators, requiring investment in advanced technology and constant adaptation of strategies[2].

An important aspect is that the burden of proof for removing fake reviews often falls on the businesses themselves. Although platforms are slow to respond to complaints about fake reviews, it is often the affected business that is responsible for proving fraud. This creates a significant operational and financial burden for businesses that follow the rules. This asymmetry means that those engaging in unfair practices face less immediate risk and cost, while their victims bear significant costs and reputational damage. This can lead to a 'race to the bottom' where businesses may be tempted to use similar tactics to survive, further polluting the market and undermining the very purpose of consumer feedback.

- **Methods for detecting fake reviews and bots.** Various detection methods are used to combat review and rating manipulation:
- **Review pattern analysis:** Detection of large volumes of reviews in short periods, excessive 5-star (or 1-star) ratings, spikes coinciding with competitor actions, and duplicate or overly generic reviews.
- **Reviewer pattern analysis:** Checking accounts with minimal details or activity, account age, number of reviews, and profile completeness.
- **Linguistic analysis:** Using AI to identify semantic patterns that indicate bot-generated text, such as unusual syntax, repetition, and grammatical errors.
- **Metadata verification:** Analysis of IP addresses, geolocation, and timestamps to detect review farms.
- **Honeypot strategy:** Creation of fictitious offers to attract fake reviewers and subsequent analysis of their patterns.
- **Reviewer verification:** Manually contacting and verifying suspicious reviewers with a large number of reviews to confirm their authenticity.
- **Deterrence:** Actively monitoring, reporting, and taking legal action against confirmed fake reviewers. The proposed FTC rules make fake reviews illegal, with significant penalties.
- **Proactive platform policies:** Encouraging platforms to continuously improve their mechanisms for detecting fake reviews through technology and human oversight.

[1]LocalConsumerReviewSurvey 2023 URL:https://www.brightlocal.com/research/local-consumer-review-survey-2023/
[2]Fake Reviews: A Growing Threat to Trust in the Digital Marketplace URL:Fake Reviews: A Growing Threat to Trust in the Digital Marketplace - Center for Digital Society

• **Review management platforms:** Use specialised platforms that help brands monitor, manage, and respond to reviews, with some using NLP to identify trends and sentiments.

• **Consumer tools:** AI-powered tools such as the FakeSpot browser extension are available to help consumers identify fake reviews on their own.

• **Monitoring for abnormal spikes:** Tracking unusual spikes in discussion or sudden shifts in sentiment related to the industry on forums and social media.

• **Account metadata tracing:** Examining account metadata such as profile creation dates, amount of content posted, and geolocation to identify bot networks.

• **Reverse image search:** Using Google reverse image search to determine the origin of images used by suspicious bot accounts.

• **Digital watermarking:** Considering the possibility of digitally watermarking your own content so that copies altered by bots remain tied to the original source.

• **Abuse of dominant position in the digital services market (self-preferencing, access restrictions).**

• **Definition of dominant position and its characteristics in digital markets.** Dominant position in the digital services market is often linked to the concept of 'gatekeepers' as defined by the European Union's Digital Markets Act (DMA). Gatekeepers are large digital platforms that offer certain 'core platform services' such as online search engines, app stores and messaging services. To be defined as a gatekeeper, a company must meet several criteria: have a strong economic position and significant influence on the internal market, operate in many EU countries; occupy a strong intermediary position, i.e. connect a large user base with a large number of businesses; and have an established and sustainable market position, meaning that their position has remained stable over a long period of time. As of 6 September 2023, the European Commission has identified six companies as gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft[1]. The peculiarities of a dominant position in digital markets are that access to and control of user data can further strengthen the power of these platforms over various aspects of business-consumer relations.

Platforms often benefit from network effects, where the value of the platform increases as the number of users grows, creating a 'winner takes all' effect. In addition, they enjoy economies of scale, achieving efficiency by providing multiple services simultaneously.

• **Self-preferencing. Self-preferencing** is the practice of a digital platform favouring its own products or services over those of its competitors. This can manifest itself in various ways:

· **Prioritisation in search results:** Google may favour video content hosted on YouTube (an Alphabet asset) or give higher rankings to companies that have paid for it.

· **Selectivity in marketplaces:** Searching for a product on Amazon, such as a toaster, may favour Amazon's own brand, Amazon Basics, by placing it first in the list.

· **Default services:** A manufacturer of mobile phones running Android (a Google product) may make Google Search the 'default' search engine on a new device. Although users can download other search engines, the 'default' status is extremely valuable, as evidenced by Alphabet's annual payment of $12 billion to Apple for the status of default search engine on the iPhone.

· **Restrictions in app stores:** Apple, for example, restricts the sale of iPhone apps to its own App Store, where it charges a significant commission.

• The Digital Markets Act (DMA) explicitly prohibits gatekeepers from favouring their own products or services in rankings over similar services or products offered by third parties on their platform. They must also allow their business users to promote their offers and enter into contracts with their customers outside the gatekeeper's platform. These provisions aim to ensure a fair business environment for business users who depend on gatekeepers.

• Antitrust authorities have long been investigating such practices. The European Commission, for example, fined Google €4.34 billion for abusing its dominant position through self-preferencing in its Android practices.[2] Amazon has also faced antitrust scrutiny over its treatment of third-party sellers on its platform. The DMA, by introducing *ex ante* regulation, is a direct response to the limitations of *ex post* enforcement in dynamic digital markets. This underscores that regulators recognise the need for preventive measures to ensure competitiveness.

[1]Commission designates six gatekeepers under the Digital Markets Act URL:https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en

[2]Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine URL:.https://ec.europa.eu/newsroom/comp/items/631884/

- **Restriction of Access. Restriction of access** is a practice whereby a dominant platform uses its control to restrict or prevent competitors from accessing the market or its services. This can manifest itself in the form of:
- **Prohibiting contact with businesses outside the platform:** Gatekeepers cannot prevent consumers from contacting businesses outside their platforms.
- **Restrictions on software removal:** Gatekeepers must not prevent users from removing any pre-installed software or apps if they wish to do so.
- **Forced use of payment systems:** Gatekeepers cannot force app developers to use their own payment systems for in-app purchases, but must allow the use of third-party payment systems.
- **Unfair conditions for app developers:** Gatekeepers cannot impose unfair conditions on app developers for access to their app stores.
- The DMA sets out clear obligations for gatekeepers to ensure fair access and interoperability. They must allow third parties to interact with their services in certain defined situations. Gatekeepers are also required to provide their business users with access to data generated through the use of the gatekeeper's platform on fair, reasonable and non-discriminatory terms. For messengers, this means that gatekeepers must ensure the interoperability of their messaging services with third-party services.

Digital markets are often characterised by network effects, where the value of the platform increases as the number of users increases, which can create a 'winner takes all' environment. This creates challenges for new market entrants, as it is difficult for them to overcome existing barriers to entry, which strengthens the position of established players.

- **Impact on competition, innovation and consumers.** Abuse of a dominant position, including self-preferencing and access restrictions, has a significant negative impact on competition, innovation and consumers. It leads to reduced innovation, as smaller firms and start-ups face barriers to competition and growth. Consumers may face higher prices due to a lack of competition and have less choice of services. It can also lead to a market where it is difficult for new entrants to compete, leading to monopolistic behaviour.
- The Digital Markets Act (DMA) aims to counteract these negative effects. It creates a fairer business environment for business users who depend on gatekeepers. Innovators and tech start-ups gain new opportunities to compete and innovate without unfair conditions that limit their development. Consumers get more and better services to choose from, more opportunities to switch providers, and fairer prices.
- Failure to comply with DMA obligations can have significant consequences for gatekeepers, including fines of up to 10% of the company's total annual worldwide turnover (up to 20% in the case of repeated infringements) and periodic penalty payments of up to 5% of average daily turnover. In the event of systematic violations, additional measures may be imposed, including non-financial measures such as divestiture of parts of the business. The DMA also aims to address the problem of regulatory fragmentation caused by national legislative initiatives in EU member states, which previously led to increased compliance costs for cross-border platforms. The new rules provide clearly defined obligations for gatekeepers, while smaller players and start-ups are not subject to these rules but benefit from fairer behaviour when interacting with gatekeepers.

The impact of AI on competitive behaviour (algorithmic collusion). Definition and forms of algorithmic collusion.

- **Algorithmic collusion** is a phenomenon where algorithms are used to coordinate prices, production volumes or other competitive variables between firms, thereby restricting competition[1]. This is one of the most pressing issues in the context of the growing dependence of markets on AI for price setting, especially in digital markets.[2]
- Algorithmic collusion can take various forms:
- **Price-fixing:** Algorithms can be used to set prices at a certain level, eliminating price competition between firms.
- **Market allocation:** Algorithms can be used to allocate markets or customers between firms, reducing competition.
- **Output restriction:** Algorithms can be used to restrict output, thereby reducing supply and increasing prices.

[1]Sarah Lee Algorithmic Collusion in Antitrust URL:Algorithmic Collusion in Antitrust
[2]Maria GiacaloneAlgorithmic Collusion: Corporate Accountability and the Application of Art. 101 TFEU. URL:Algorithmic Collusion: Corporate Accountability and the Application of Art. 101 TFEU | European Papers

- Algorithms play a crucial role in pricing, output, and other business decisions in the digital economy. They can facilitate collusion by monitoring and enforcing collusive agreements, coordinating prices and production volumes, and adapting to changes in market conditions.
- **Mechanisms and examples.** Algorithmic collusion mechanisms rely on the use of complex algorithms that process large amounts of data to make decisions.
- **Pricing algorithms:** These algorithms use data on prices, demand, and other market variables to set prices.
- **Machine learning algorithms:** These algorithms use data to learn patterns and make predictions that can be used to facilitate collusion.
- Examples of algorithmic collusion include:
- **Topkins case:** In 2016, the US Department of Justice fined David Topkins, CEO of a poster manufacturing company, for using algorithms to fix prices.
- **The Trod case:** In 2018, the UK Competition and Markets Authority fined Trod, an online poster sales company, for using algorithms to fix prices.
- **RealPage Inc. case:** The US Department of Justice has expressed concern about the use of third-party pricing algorithms, notably in a case against RealPage Inc., whose AI-based pricing tools for rental housing allegedly facilitated collusion between landlords. Similar lawsuits have been filed against pricing tools in the hotel and rental industries, indicating a shift in the focus of antitrust law toward algorithmic pricing in various industries.

An important issue is so-called 'tacit collusion' or 'parallel behaviour,' where algorithms can coordinate the market behaviour of competitors without explicit human agreements. This occurs when each firm uses its own pricing algorithm, and although there is no initial or ongoing communication between the companies, the algorithms can autonomously achieve goals that lead to anti-competitive outcomes.

Challenges for antitrust law and regulation. The growing reliance on AI in pricing poses significant challenges to existing antitrust frameworks, which have traditionally been based on the assumption that collusion is a human-driven process.

Key challenges include:

- **Lack of transparency:** Algorithms can be complex and opaque, making it difficult to detect collusion.
- **Lack of intent:** Algorithms can facilitate collusion without human intent, making it difficult to establish liability. This is a fundamental challenge to the legal concepts of 'collusion' and 'liability,' as traditional law requires proof of intent. When an algorithm acts autonomously to achieve an anti-competitive outcome, the question arises as to whether this intent can be attributed to the company that developed or uses it. This requires a reassessment of the existing legal framework.
- **Lack of jurisdiction:** Algorithmic collusion may involve firms from multiple jurisdictions, making enforcement coordination difficult.
- There is debate among academics as to whether antitrust law should be stricter or, conversely, more lenient in response to AI technology. There are also concerns about predatory pricing, which may be facilitated by AI, allowing firms to minimise losses and recoup costs more efficiently. Regulators need to review the counterfactual assessments used to determine pricing conditions in the absence of collusive behaviour so that they reflect the capabilities of AI-based algorithmic pricing.
- For businesses using algorithmic pricing, the following measures are recommended to mitigate risks:
- **Review and audit algorithmic pricing models:** Document that the use of AI and algorithmic pricing is only one factor in determining a fair price, and regularly check algorithms for coordination risks.
- **Implement strict monitoring and control:** Ensure automated tracking systems and human oversight for algorithm operation, monitor price adjustments in real time, and maintain audit logs for pricing decisions.
- **Maintain thorough documentation:** Keep records that explain how pricing models function and why specific decisions are made, including logs of decisions regarding algorithm development and updates.
- **Avoiding customer mistrust:** Consider the transparency of algorithmic pricing tools, as disclosure of such information may alienate potential customers who perceive the technology as manipulative or unfair.
- The concept of AI as an 'extension' of a business is becoming increasingly important for ensuring accountability. If an algorithm performs its functions for and under the direction of a business, it is integrated into the economic unit of the business, and the company is responsible for its actions, similar to the actions of an employee.[1]

[1]Androschuk G.O. Artificial intelligence and intellectual property: problems of regulation: scientific and practical publication. Research Institute of Intellectual Property of the National Academy of Sciences of Ukraine. Kyiv: Interservice, 2023.- 204 p. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0a3ae7df-6993-490d-9eae-d5a6d1cab8d1/content

3. Ukrainian context: Legislation and regulation.

General provisions of Ukrainian competition law. In Ukraine, issues of protection against unfair competition and antitrust regulation are governed by Article 42 of the Constitution, the Laws of Ukraine 'On Protection against Unfair Competition,' 'On Protection of Economic Competition,' and 'On Protection of Consumer Rights.' Although these laws do not directly define 'digital markets,' they prohibit a number of anti-competitive practices. These include abuse of a monopoly position in the market, which may lead to a restriction of competition or harm to consumers, as well as anti-competitive concerted practices. The Law of Ukraine 'On Protection of Consumer Rights' establishes new approaches to the interpretation of unfair commercial practices and defines the criteria for determining whether a commercial practice is unfair, as well as the definition, types and regulation of misleading commercial practices. The new law significantly strengthens regulation in this area of consumer protection and establishes increased requirements and restrictions for business entities. Another positive development is the definition of an exhaustive list of types of aggressive commercial practices.

Separately, the law prohibits unfair competition, which includes the unlawful use of business reputation, the dissemination of false information, and the creation of obstacles to the activities of competitors. These rules are aimed at promoting transparency and preventing actions that may restrict competition, such as price manipulation or the creation of monopoly conditions in the market.

Regulation of digital services and content. On 7 March 2024, the Law of Ukraine 'On Digital Content and Digital Services' came into force in Ukraine. [1] This law defines key concepts in the field of digital products:

Digital content: Data created and provided in digital form, including computer programs, applications, video and audio files, music files, digital games, and e-books.

Digital services: Services that enable consumers to create, process, store and distribute data in digital form or to access such data. These include cloud services, social networks, video streaming services (e.g. Netflix or Spotify).

The law applies to relationships in which digital content and/or digital services are developed according to the consumer's specifications, as well as to relationships in which the contractor provides digital content on a physical medium used exclusively for storing such content. Companies operating in this field are required to review their terms and conditions, implement policies that guarantee product quality, and provide customer support in case of problems. Another important requirement is to provide updates for products to ensure their security and functionality.

Challenges of antitrust regulation of digital platforms in Ukraine. Digital platforms, algorithms, and big data are the new reality of the global digital economy. Major players in the digital platform market use the innovative environment to secure a dominant position in the market. The use of advanced technologies allows companies to impose unfair conditions on consumers, expand their market power, raise prices and close markets to potential competitors.

The new model of market competition in the digital economy requires the use of qualitatively new regulatory tools and the improvement of existing methods of protecting competition. Recently, the Ministry of Digital Transformation launched Digital State UA, a platform for digital Ukraine. The platform showcases Ukraine's achievements in GovTech, IT and Tech. Unfortunately, Ukrainian lawmakers have not yet paid sufficient attention to the problems of digital platform functioning. The dominance of global digital platforms and the lack of 'national' platforms in Ukraine puts Ukrainian entrepreneurs at a disadvantage, creating the risk that Ukrainian retail chains will lose contact with Ukrainian consumers. There is a threat of market monopolisation by global digital monopolies using powerful digital platforms and the displacement of smaller players.[2]

As noted by Butnik-Siverskyi O.B., "The development of the digitalisation of the intellectual property economy in the context of digital platforms, as a feature of the human-digital system, requires fundamental changes in the general approaches to the legal regulation of a new type of economic relations, since the

[1] On digital content and digital services. Law of Ukraine dated 10.08.2023 No. 3321–IX. Verkhovna Rada of Ukraine. Legislation of Ukraine. URL: https://t.ly/o__DJ.

[2] Intellectual property in the digital economy: problems of theory and practice (collective monograph) edited by Candidate of Economic Sciences, Associate Professor G.O. Androschuk. Kyiv: Interservice, 2025. 452 p. URLhttps://drive.google.com/file/d/16xDa1LRj52vOFVJv6oYVaIptpNtyvDoF/view

activities of digital platforms affect both public (financial, tax) and private law (civil, commercial, labour) matters." [1]

The Antimonopoly Committee of Ukraine (AMCU) recognises the need to adapt competition legislation. In October 2023, the AMCU defined a vector for analysing product market boundaries in the presence of buyer market power (monopsony), reflecting international experience and developments in competition legislation. This demonstrates an understanding that antitrust authorities around the world are improving their tools and methodologies for combating anti-competitive practices, and Ukraine is also joining this process by expanding its understanding of market power beyond traditional monopolies. The authors propose the models hownin Fig. 2.

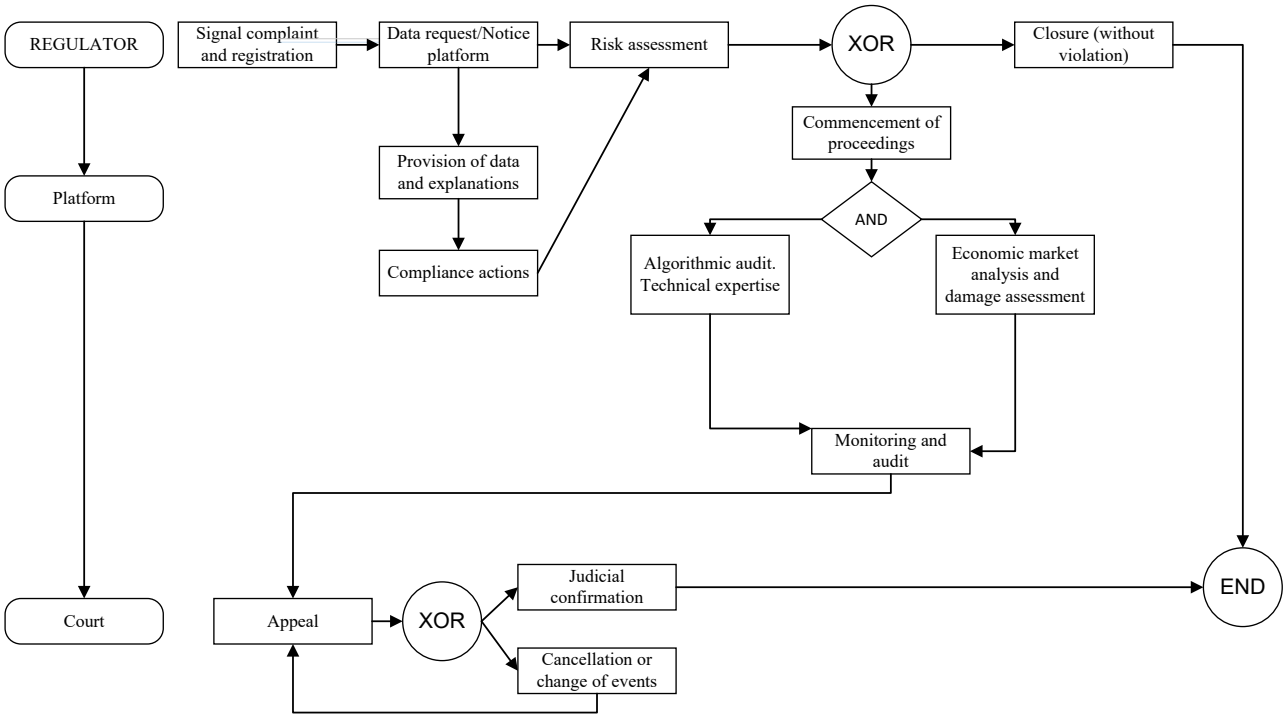


Fig. 2. *Model of antitrust control in the digital economy*

Conclusions. Unfair competition in the digital economy is becoming algorithmic and platform-infrastructure-based in nature, which significantly distinguishes it from traditional forms of anti-competitive behaviour. Digital platforms, combining control over data, ranking algorithms and network effects, are forming a new configuration of market power capable of influencing not only the structure of competition, but also the information environment and consumer behaviour.

The study allowed us to formulate the following key conclusions.

1. **Algorithmisation of unfair competition.**

Modern practices of distorting competition are implemented through algorithmic mechanisms — self-prioritisation, visibility manipulation, automated pricing, algorithmic coordination, and opaque data access management. This indicates a shift from behavioural to infrastructural-algorithmic forms of anti-competitive influence.

2. **The dual role of digital platforms.**

Digital platforms reduce transaction costs and stimulate innovation, but their ability to accumulate large amounts of data and reinforce network effects creates the conditions for market power concentration and

[1]Butnik-Siversky, O.B. Digital platforms on the path to digitalization of the intellectual property economy // Improving legislation and the mechanism for implementing the protection of intellectual property rights in the conditions of post-war reconstruction of Ukraine. Section 6. “Project management. Prospects for the development of project and neuromanagement, information management technologies, technologies for creating and using intellectual property objects, technology transfer”: collection of scientific papers based on the materials of the V International Scientific and Practical Internet Conference, March 23–24, 2023 – Kyiv, 2023. – P. 29-32. URL https://dspace.nuft.edu.ua/items/da76854c-f835-4922-af60-0e94318e03aa

information asymmetry. Such concentration can transform into systemic barriers to entry and mechanisms of unfair competition.

3. **Transformation of the regulatory paradigm.**

The evolution of competition regulation demonstrates a shift from a reactive (ex post) to a preventive (ex ante) model, which is reflected, in particular, in European practice of regulating digital markets. This confirms the need for early detection of algorithmic risks and the introduction of structural and behavioural restrictions before irreversible market consequences arise.

4. Challenge to traditional concepts of liability.

Algorithmic coordination and autonomous decision-making by artificial intelligence systems call into question classical approaches to proving conspiracy and intent. This requires a review of the doctrine of liability, taking into account the role of algorithm developers, platform operators and data owners.

5. **Erosion of trust as a factor in market concentration.**

Manipulation of reviews, SEO spam and other forms of information distortion not only undermine consumer trust, but also contribute to the consolidation of the dominance of large platforms by reducing the transparency of market alternatives.

6. **National dimension of regulation.**

Ukrainian legislation is gradually adapting to digital challenges, but needs further systematisation and harmonisation with European competition policy standards. The development of mechanisms for algorithmic auditing, platform transparency and strengthening the institutional capacity of competition control authorities is particularly relevant.

7. **Conceptual outcome of the study.**

The paper develops an economic and legal model for regulatory countermeasures against algorithmic mechanisms of unfair competition, integrating tools for risk identification, legal qualification, proportionate application of enforcement measures, and further monitoring of implementation. The proposed approach allows a transition from a fragmented response to a system of digital antitrust control.

Overall, ensuring fair and open digital markets requires a comprehensive approach that combines legislative adaptation, the development of abuse detection technologies, increased transparency of algorithmic systems, and active international coordination. The formation of such a system is a prerequisite for preserving a competitive environment, stimulating innovation, and protecting the economic security of the state.

REFERENCES

1. Bodenhausen, G. (2018). *Paris Convention for the protection of industrial property: Commentary* (G. O. Androschuk, Trans., Preface & Sci. ed.). Parliamentary Publishing House.
2. Androschuk, G. O., & Shklyar, S. V. (2012). *Competition law: Protection against unfair competition*. Justinian.
3. Vinnyk, O. M. (2021). *The law of the digital economy*. Research Institute of Private Law and Entrepreneurship named after Academician F. H. Burchak of the National Academy of Law Sciences of Ukraine. https://t.ly/osxVj
4. European Commission. (n.d.). *The Digital Markets Act*. https://digital-markets-act.ec.europa.eu/index_en
5. Polyukhovich, V. (2024). Protection of economic competition in digital markets in Ukraine. *University Scientific Notes, 5*(101), 17–30. https://doi.org/10.37491/UNZ.101.2
6. Trajcheva, S. (n.d.). *What is SEO spam and how does it impact your site?*
7. Winston, A. R. (n.d.). *10 SEO spam types & how to avoid: Personal injury lawyers*.
8. BrightLocal. (2023). *Local consumer review survey 2023*. https://www.brightlocal.com/research/local-consumer-review-survey-2023/
9. Center for Digital Society. (n.d.). *Fake reviews: A growing threat to trust in the digital marketplace*.
10. European Commission. (2023, September 6). *Commission designates six gatekeepers under the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en
11. European Commission. (n.d.). *Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine*. https://ec.europa.eu/newsroom/comp/items/631884/
12. Lee, S. (n.d.). *Algorithmic collusion in antitrust*.
13. Giacalone, M. (n.d.). *Algorithmic collusion: Corporate accountability and the application of Art. 101 TFEU*. *European Papers*.
14. Androschuk, G. O. (2023). *Artificial intelligence and intellectual property: Problems of regulation*. Research Institute of Intellectual Property of the National Academy of Sciences of Ukraine; Interservice. https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0a3ae7df-6993-490d-9eae-d5a6d1cab8d1/content
15. Law of Ukraine No. 3321–IX, On digital content and digital services (2023, August 10). *Verkhovna Rada of Ukraine. Legislation of Ukraine*. https://t.ly/o__DJ
16. Androschuk, G. O. (Ed.). (2025). *Intellectual property in the digital economy: Problems of theory and practice*. Interservice. https://drive.google.com/file/d/16xDa1LRj52vOFVJv6oYVaIptpNtyvDoF/view
17. Butnik-Siversky, O. B. (2023, March 23–24). Digital platforms on the path to digitalization of the intellectual property economy. In *Improving legislation and the mechanism for implementing the protection of intellectual property rights in the conditions of post-war reconstruction of Ukraine* (Section 6, pp. 29–32). Collection of scientific papers based on the materials of the V International Scientific and Practical Internet Conference, Kyiv, Ukraine. https://dspace.nuft.edu.ua/items/da76854c-f835-4922-af60-0e94318e03aa