Artificial Intelligence in Consumer Rights Protection: New Opportunities and Legal Challenges

[1]Ferents Filip
[1]Expert in Consumer Rights Protection and the Application of Artificial Intelligence in Legal Processes
Founder of an AI-powered platform designed to protect consumer rights and automate legal processes in the U.S. home services and digital services industries
Williamsburg, Va USA

Abstract

The incorporation of artificial intelligence (AI) into consumer markets initiates a genuine paradigmatic shift, revealing a tense dialectic between the empowerment of consumers and the emergence of unprecedented legal and ethical threats. The aim of the article is to provide a systematized analysis of this duality, covering both the positive effects of AI deployment (hyperpersonalization, preventive anti-fraud measures, online dispute resolution) and the risks inherent in the technology—algorithmic bias, manipulative practices, and the undermining of decisional autonomy. The methodological framework relies on a systematic review of scholarly and regulatory literature and a comparative legal analysis of key European Union instruments—the Artificial Intelligence Act (EU AI Act) and the new Product Liability Directive (PLD). The findings indicate that AI provides transformative tools for enhancing the efficiency and accessibility of consumer protection mechanisms; at the same time, the very same technological capabilities generate systemic risks of nonobjectivity and dilute the informed nature of decision making. The new European regulation establishes an advanced risk-based architecture, rethinking the allocation of responsibility and imposing preventive obligations on providers of AI systems, while simultaneously complicating enforcement. In conclusion, the paper substantiates the need for a balanced course that combines technological safeguards, proactive regulatory oversight, and the development of consumer digital literacy for the harmonious development of the digital economy. The presented conclusions are addressed to legal scholars, regulators, developers, and compliance professionals involved in AI governance.

1. Introduction

The contemporary digital economy is marked by the pervasive and rapid diffusion of artificial intelligence (AI) technologies across consumer sectors. This process radically transforms established patterns of business–consumer interaction while simultaneously creating new market niches and increasing the efficiency of existing ones. The relevance of the topic is determined by the scale and pace of these transformations: as of 2024, the volume of the e-commerce market using AI will reach 7,57 billion USD, and by 2025 it will grow to 8,65 billion USD [1]; accompanying investment activity is also accelerating—by 2025, global investments in AI may reach billion USD [3]. It is expected that by the end of 2025 more than 80% of retail executives will have implemented AI-based automation solutions in their organizations [2].

The Am. J. Polit. Sci. Law Criminol. 2025

7

Despite the evident benefits—productivity growth and deepened personalization of the customer experience—the integration of AI gives rise to a cluster of problems at the intersection of law, ethics, and technology. On the one hand, AI expands consumer capabilities by improving service quality, enhancing safety, and introducing new protection mechanisms. On the other, it generates significant risks, including algorithmic bias, decision-making opacity, behavioral manipulation, and threats to data confidentiality [4]. The academic literature notes a deficit of systematized syntheses on the ethical constraints and vulnerabilities in the use of AI in marketing and consumer interaction, which underscores the need for an interdisciplinary, comprehensive analysis [4].

The aim of this study is to carry out a comprehensive legal and ethical analysis of the impact of AI on the system of consumer rights, with special attention to the emergence of the European regulatory architecture as a potential benchmark for global regulation.

The working hypothesis is that classical legislation formed in the pre-algorithmic era is insufficient to provide an adequate response to the specific challenges generated by AI. Hence the need for proactive, risk-oriented regulatory models such as the European AI Act; at the same time, their implementation in itself creates new problems of law enforcement, allocation of liability, and maintaining a balance between protection and innovation.

The scientific novelty of the work lies in a holistic consideration of the complementary effect of two key EU acts—the AI Act and the revised Product Liability Directive—as a single protective framework for consumer rights in the age of algorithmization.

2.   Materials and methods

The methodological architecture of the study is integrative and designed to ensure a comprehensive consideration of the stated problem domain. The analytical strategy relies on a set of mutually complementary approaches.

First, a systematic literature review was conducted covering peer-reviewed corpora Scopus, Web of Science, IEEE Xplore, and SpringerLink. The purpose of the review was to map the current scholarly discourse in the areas of AI ethics, algorithmic bias, legal challenges, and the transformation of consumer behavior under the influence of digital technologies.

Second, the core method was comparative legal analysis. The objects of detailed examination were primary normative sources, including the final texts of Regulation (EU) 2024/1689 (Artificial Intelligence Act) and Directive (EU) 2024/2853 (new Product Liability Directive). The analysis was oriented toward identifying key legal mechanisms, the logic of their interaction, and possible implications for the status and protection of consumer rights.

Third, a case study analysis method was employed for empirical illustration of the theoretical propositions. Documented cases and industry reports on AI application practices were examined — in particular, dynamic pricing (the Uber case) and online dispute resolution — which made it possible to link the theoretically described risks with examples observed in reality.

3.   Results and Discussion

The deployment of artificial intelligence technologies in the consumer domain creates a substantial potential to strengthen consumer protection mechanisms, raise service quality standards, and expand as well as reduce the cost of access to justice. These effects materialize across a number of key areas in which AI functions as a systemic driver of transformation.

AI algorithms are radically transforming the architecture of e-commerce, shifting the emphasis from mass communications to a mode of hyper-personalized interactions. By analyzing large volumes of behavioral data and user preferences, such systems generate targeted product recommendations, which improves the quality of the user experience [4]. Empirical metrics confirm the effectiveness of the approach: AI tools make it possible to identify consumer trends 30% faster and increase the accuracy of forecasts by 25% relative to traditional methods [5]. For consumers, this results in reduced time to find a relevant product and higher relevance of the proposed options: users interacting with AI assistants' complete purchases 47% faster, and conversion rates in online stores with AI chats can increase fourfold [19]. Consequently, AI simultaneously optimizes the operational contours of businesses and enhances efficiency as well as consumer satisfaction.

One of the key consumer vectors of AI application is the strengthening of financial security. AI algorithms are

capable, in real time, of traversing datasets comprising millions of payments, isolating statistical anomalies and atypical behavioral signatures indicative of probable fraud [21]. Such predictive diagnostics enables the preemptive blocking of suspicious transactions, thereby protecting citizens' assets before actual damage occurs. The scale of practical effectiveness is corroborated by public-sector experience: in 2023, the U.S. Department of the Treasury, using AI-based fraud detection tools, recovered more than 375 million dollars [21]. For consumers, this translates into increased trust in digital payment systems and reduced risks associated with online transactions.

Artificial intelligence is also redefining dispute resolution procedures, making access to justice faster and more cost-effective. AI-enhanced online dispute resolution (Online Dispute Resolution, ODR) platforms are becoming an effective alternative to traditional litigation, especially in the small-claims segment, which previously often remained unresolved due to disproportionate costs [23]. Empirical evidence confirms the effectiveness of such solutions: the eBay platform resolves more than 60% of disputes without human involvement [25], while Canada's PARLe-OPC achieves settlement in 70% of cases [23]. AI integration makes it possible to reduce processing times by up to approximately 50% [24]. Market dynamics—the forecast for the digital arbitration segment at 28.33 billion U.S. dollars by 2025 [20]—indicate strong demand and substantial potential of such technologies for the systemic strengthening of consumer protection.

In this way, AI ceases to be merely a means of optimizing commercial processes and, in effect, constructs a new infrastructure for the enforcement and protection of consumer rights, enhancing the efficiency, safety, and accessibility of justice in the digital legal space. This simultaneously heightens the demands for fairness, transparency, and impartiality of the relevant institutions.

Despite all the evident advantages, large-scale integration of AI gives rise to serious legal and ethical challenges capable of undermining fundamental consumer rights. The paradox is that the mechanisms that generate positive effects simultaneously serve as a source of key risks.

Algorithmic bias — one of the most severe and empirically substantiated AI risks — arises when a system reproduces or amplifies social stereotypes embedded in the training data, or when the very design of the model is defective [12]. The consequence is systematic discrimination against certain groups of consumers in critically important domains — from credit scoring and insurance to employment and access to housing.

Algorithmic pricing (dynamic price discrimination) is a distinct cause for concern. Drawing on large-scale behavioral datasets (browsing history, geolocation, device type), AI algorithms set personalized prices based on assessed solvency or willingness to pay. Such practices undermine the principle of equal access to goods and services and are perceived as unfair, thereby reducing overall consumer welfare. The example of Uber is illustrative: the company was accused of using algorithms to set higher rates in high-income neighborhoods — a vivid demonstration of the risk described [9].
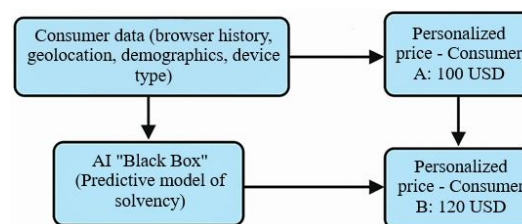

Fig. 1. Conceptual diagram of algorithmic price discrimination (compiled by the author based on [9]).

As shown in Fig. 1, the ability of AI to process colossal volumes of personal data, enabling hyperpersonalization (advantage), is inextricably linked with the capability for fine-grained consumer segmentation for discriminatory pricing (risk). This confirms that AI risks are not a side effect of use but a constitutive, immanent characteristic of the technology itself, requiring not targeted bans on undesirable outcomes but comprehensive regulation of the entire life cycle of the AI system.

Many contemporary AI systems, especially those based on deep learning, operate as black boxes: their internal logic is so complex that it remains opaque even to developers. Such epistemic opacity and lack of explainability create serious obstacles to consumer protection [6]. When a consumer is denied a loan, has an insurance premium increased, or is rejected for a job on the basis of an AI decision, they are effectively deprived of the ability to understand the rationale and, consequently, to contest the outcome effectively. The

The Am. J. Polit. Sci. Law Criminol. 2025

9

absence of transparency likewise complicates regulatory efforts to establish accountability for erroneous or discriminatory decisions.

AI can also be used for sophisticated manipulative practices that undermine consumer autonomy: from dark patterns in interfaces that steer users toward disadvantageous choices to more complex psychographic targeting campaigns. Such systems are capable of identifying and exploiting cognitive vulnerabilities — related to age, financial status, or psychological condition — for the purpose of significant distortion of behavior, which may entail substantial harm [7]. These practices inflict direct economic damage and erode the foundation of market relations — the principle of informed and free choice.
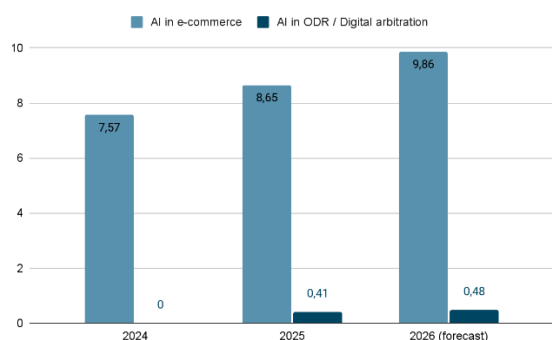

Fig. 2. Forecast for growth of AI markets in e-commerce and online dispute resolution (2024–2026)

(compiled by the author based on [1, 7]).

The rapid dynamics of markets, as shown in Fig. 2, render the stated risks particularly acute. The mass integration of AI simultaneously into commercial products and into the dispute-resolution mechanisms arising from those same products creates a self-reinforcing feedback loop: as capabilities expand, vulnerabilities increase. The result is a governance gap: technological innovations are deployed faster than legal norms and enforcement practice can respond. It is indicative that the key provisions of the EU AI Act for high-risk systems will take effect only in June 2026, leaving consumers in a state of heightened exposure to risks during the transition period [15].

In response to these challenges, the European Union has developed a coherent regulatory architecture that aspires to serve as a global reference point for AI regulation. It rests on two complementary components: preventive (the AI Act) and compensatory (the new Product Liability Directive), ensuring a combination of ex ante requirements and ex post liability.

The EU Artificial Intelligence Act (EU AI Act) establishes horizontal, cross-sectoral rules based on a risk-based approach. AI systems are differentiated into four risk levels, and the set of regulatory requirements varies in accordance with this classification (see Table 1) [7].

Table 1. Classification of risks and key obligations under the EU AI Act in the context of consumer protection (compiled by the author based on [7, 13]).

Risk level	Examples relevant to consumers	Key obligations	Protected consumer right
Unacceptable	Social scoring systems; manipulative systems causing harm; exploitation of vulnerabilities.	Total prohibition.	The right to autonomy, dignity, freedom from manipulation.
High	Credit scoring; assessment of access to education and employment; biometric identification; safety components in products.	Risk management system; data governance; technical documentation; human oversight; cybersecurity; registration in the EU database.	The right to non-discrimination, equality, access to information, safety.

The Am. J. Polit. Sci. Law Criminol. 2025

10

Limited	Chatbots; emotion recognition systems; deepfakes.	Transparency obligation (the user must be informed that they are interacting with AI or viewing generated content).	The right to receive accurate information.
Minimal	Spam filters; AI in video games.	Voluntary adherence to codes of conduct.	(Indirectly) The right to privacy.

For the protection of consumer rights, the regimes of unacceptable risk and high risk are key. A direct ban on manipulative and exploitative solutions addresses threats of undermining consumer autonomy. The classification of credit scoring systems and mechanisms determining access to basic services as high-risk imposes strict preventive obligations on their providers. Before such a system is placed on the market, it must undergo a conformity assessment confirming that the risks of bias are minimized, high-quality data are used, and effective mechanisms of human oversight function. Non-compliance with these requirements entails significant sanctions — up to 35 million euros or 7% of the company's worldwide annual turnover [15].

If the AI Act performs the role of a preventive shield, the new Product Liability Directive (PLD), to be implemented into the national legal orders of EU Member States by December 2026, is a compensatory sword. It modernizes the liability regime for damage caused by defective products, adapting it to the conditions of the digital age.

The Directive carries out a comprehensive modernization of the liability regime for defective products, adapting it to the digital economy and the circulation of AI. The adopted provisions close previous regulatory lacunae, specify the allocation of procedural functions among participants, and strengthen the compensatory potential of tort protection of the consumer within the jurisdiction of the EU [14, 16].

First, the very category of product is rethought: software — including AI systems and their updates — is expressly recognized as a product. This removes the gap that had created systemic barriers to holding software developers liable; the corresponding regime also extends to intangible digital objects that participate in supply and operational chains.

Second, the principle of strict (no-fault) manufacturer liability is preserved: to obtain compensation the consumer is not required to prove fault. It is sufficient to establish the existence of a defect in the goods (including software), the fact of harm suffered, and a causal link between them. This model supports predictability and reduces the procedural costs of the injured party [10, 11].

Third, the rules of evidence in technologically complex disputes, including claims involving AI, have been transformed. Courts are empowered to compel the manufacturer to disclose relevant technical documentation; moreover, a rebuttable presumption of defect or causation is introduced if the manufacturer evades disclosure of the necessary data or when the defect is clearly attributable to a breach of safety requirements [8]. These instruments reduce the black-box effect typical of highly complex algorithmic systems.

Finally, the circle of potentially liable parties is expanded: in addition to manufacturers, importers, authorized representatives, and in certain cases online platforms may be held liable [8]. An extended chain of responsibility is formed, ensuring the presence of an appropriate defendant within the EU and increasing the practical enforceability of consumer claims [18, 22].

Accordingly, it can be stated that the new regulatory acts do not operate in isolation; they are embedded in the existing fabric of European law, forming a multi-level protective framework. The AI Act serves as a specialized complement to the Unfair Commercial Practices Directive (UCPD), enshrining more detailed prohibitions on manipulative technological techniques. Its data-governance requirements are conceptually aligned with the General Data Protection Regulation (GDPR). The key feature is their mutual reinforcement: the AI Act establishes ex ante standards of safety and fairness for AI systems prior to market placement, whereas the new

Product Liability Directive provides consumers with an enhanced mechanism for obtaining ex post compensation when preventive measures have proved insufficient [17]. This dual-circuit architecture — prevention + compensation — represents the most extensive global attempt to construct a balanced and reliable regime for AI risk governance in the interests of consumers. However, its effectiveness will be determined by the practical capacity of supervisory authorities in EU member states and by the ability of businesses, especially small and medium-sized enterprises, to adapt to complex technical and legal requirements.

To bridge the gap between high-level regulatory frameworks and practical consumer protection, the author proposes the implementation of a specialized AI-Powered Legal Platform. This system is designed to operationalize the transparency and fairness principles mandated by the EU AI Act, providing a scalable solution for the U.S. home services and digital sectors.

The platform utilizes advanced Natural Language Processing (NLP) to counter the "black box" effect and linguistic opacity in contracts. By automating the detection of dark patterns and hidden clauses, the system directly addresses the risks of manipulative practices identified earlier in this study.

The architecture consists of three core modules aligned with the mission to democratize access to justice:

Contract Analysis Engine: Automatically highlights unfair terms and explains them in plain language, increasing legal literacy.

Safe Contract Generation: Standardizes agreements for small businesses to prevent future disputes.

Legal Navigator: A "What to do if..." interactive guide that empowers users to resolve disputes without litigation.

To ensure the solution effectively reaches vulnerable populations (seniors, immigrants, low-income families), a tiered access model is proposed (Table 2). This structure balances social impact with economic sustainability, offering essential protection tools at zero cost.

Table 2. Tariff plans and service costs (compiled based on the author's data)

Plan Type	Features Description	Cost (USD)
Free	Basic analysis (3 docs/month), "What to do if..." guides	$0
Standard	Advanced analysis, contract generation, secure storage	$9.99/month
Premium	Unlimited use, multilingual support, voice mode, e-signature	$29.99/month
B2B (API)	Bulk checks, integration for marketplaces	from $199/month

The development strategy is designed to validate the NLP models against regulatory standards before full-scale deployment.

Phase 1 (MVP, 6–9 months): Development of the core NLP module and testing with focus groups to ensure bias mitigation.

Phase 2 (Beta, 12–18 months): Rollout of the Contract Generator and multilingual support to aid immigrant communities.

Phase 3 (Scaling, 24–36 months): Integration of B2B APIs for marketplaces and voice mode for accessibility.

Phase 4 (Expansion, 36–48 months): Cross-border adaptation (Canada, LatAm) and government partnerships.

This roadmap reflects a proactive approach to compliance, ensuring the platform evolves alongside the regulatory landscape described in the previous sections.

4. Conclusion

The Am. J. Polit. Sci. Law Criminol. 2025

12

The conducted study confirms the central hypothesis: artificial intelligence creates for the consumer rights protection system a profound paradoxicality. On the one hand, AI acts as a powerful driver of favorable transformations, providing tools for hyperpersonalization, enhancement of financial security, and democratization of access to justice through ODR. These solutions are capable of radically improving the quality of the consumer experience and strengthening protective mechanisms. On the other hand, the same technological effects generate systemic threats — from algorithmic discrimination and the erosion of consumer autonomy through manipulative practices to the opacity of the black box.

The stated objective has been achieved through a systematic analysis of this duality and an assessment of the adequacy of the evolving regulatory architecture of the European Union. It has been established that the EU is constructing an advanced, holistic regulatory model based on the synergy of two key acts. The AI Act establishes a preventive, risk-oriented oversight system, setting strict requirements for high-risk systems even before they enter the market. The new Product Liability Directive modernizes compensatory mechanisms, simplifying for consumers the receipt of redress for harm caused by defective digital products, including AI-based solutions.

The practical significance of the study lies in the fact that, despite its complexity, the European model serves as a reference point for jurisdictions seeking a balance between the stimulation of innovation and the protection of the fundamental rights of citizens. Key conclusion: effective management of AI risks is impossible without an integrated approach that combines preventive (ex ante) and compensatory (ex post) legal instruments.

Further research should reasonably focus on issues of enforcement of the new regulation, assessment of its economic impact on small and medium-sized enterprises, and the development of technical standards in the areas of explainability, audit, and mitigation of AI bias. Ultimately, the formation of a trustworthy and fair digital environment requires continuous dialogue and cooperation among legislators, technology developers, business, and civil society.

References

1. The Future of AI In Ecommerce: 40+ Statistics on Conversational AI Agents For 2025 [Electronic resource]. - Access mode: https://www.hellorep.ai/blog/the-future-of-ai-in-ecommerce-40-statistics-on-conversational-ai-agents-for-2025 (date of access: 05.09.2025).

2. AI In eCommerce Statistics 2025 (Growth & Trends) [Electronic resource]. - Access mode: https://www.demandsage.com/ai-in-ecommerce-statistics/ (date of access: 15.07.2025).

3. 2024 Technology Industry Outlook | Deloitte US [Electronic resource]. - Access mode: https://www.deloitte.com/us/en/Industries/tmt/articles/technology-industry-outlook.html (date of access: 17.07.2025).

4. Madanchian M. The impact of artificial intelligence marketing on e-commerce sales //Systems. – 2024. – Vol. 12 (10). https://doi.org/10.3390/systems12100429.

5. Mariyappan M. S. R., Rupigaa K., Syahputra H. Revolutionizing Consumer Insights With AI and the Insight Equation: Transforming Marketing Strategies //Decoding Consumer Behavior Using the Insight Equation and AI Marketing. – IGI Global Scientific Publishing, 2025. – pp. 205-230.

6. Roy P. et al. Artificial intelligence and finance: A bibliometric review on the trends, influences, and research directions //F1000Research. – 2025. – Vol. 14. https://doi.org/10.12688/f1000research.160959.1.

7. The EU's AI Act: Review and What It Means for EU and Non-EU Companies [Electronic resource]. - Access mode: https://www.pillsburylaw.com/en/news-and-insights/eu-ai-act.html (date of access: 17.07.2025).

8. New EU Product Liability Directive Comes Into Force - Latham & Watkins LLP [Electronic resource]. - Access mode: https://www.lw.com/admin/upload/SiteAttachments/New-EU-Product-Liability-Directive-Comes-Into-Force.pdf (date of access: 25.07.2025).

9. Magazine 2023-24 - Sree Narayana Guru College Of Commerce [Electronic resource]. - Access mode: https://www.sngcollege.ac.in/uploaded_files/Magazine_23_24.pdf (date of access: 05.09.2025).

10. The Gig Trap: Algorithmic, Wage and Labor Exploitation in Platform Work in the US | HRW [Electronic resource]. - Access mode: https://www.hrw.org/report/2025/05/12/the-gig-trap/algorithmic-wage-and-labor-exploitation-in-platform-work-in-the-us (date of access:

The Am. J. Polit. Sci. Law Criminol. 2025

13

25.07.2025).

11. Hamdan R. K., Buallay A. (ed.). Artificial intelligence (AI) and customer social responsibility (CSR). – Springer, 2024. - pp. 1-5.

12. Proceedings of the 46th Annual conference of the (SAICSIT 2025) 17 - 18 July Durban Aurona Gerber [Electronic resource]. - Access mode: https://saicsit2025.org.za/online-main.pdf (date of access: 15.08.2025).

13. Pałka P., Jabłonowska A. Consumer law and artificial intelligence //Research Handbook on the Law of Artificial Intelligence. – Edward Elgar Publishing, 2025. – pp. 570-594.

14. Smuha N. A. The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. – 2025. - pp. 1-6.

15. Sillberg C. V. et al. The EU AI Act is a good start but falls short //International Conference on Software Business. – Cham : Springer Nature Switzerland, 2024. – pp. 114-130.

16. European Parliament - EU AI Act [Electronic resource]. - Access mode: https://artificialintelligenceact.eu/wp-content/uploads/2024/04/TA-9-2024-0138_EN.pdf (date of access: 25.07.2025).

17. draft Directive on liability for defective products - EUR-Lex [Electronic resource]. - Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0495 (date of access: 08.08.2025).

18. Managing gen AI risks | Deloitte Insights [Electronic resource]. - Access mode: https://www.deloitte.com/us/en/insights/topics/digital-transformation/four-emerging-categories-of-gen-ai-risks.html (date of access: 15.08.2025).

19. 40+ Latest AI in Ecommerce Statistics for 2025 [Electronic resource]. - Access mode: https://www.ecomlens.com/ai-in-ecommerce-statistics (date of access: 15.08.2025).

20. Digital Future Of Arbitration Law Market Size, Share, Growth, and Industry Analysis, By Type (Service and Software), By Application (SMEs and Large Enterprise), and Regional Insights and Forecast to 2033 [Electronic resource]. - Access mode: https://www.businessresearchinsights.com/market-reports/digital-future-of-arbitration-law-market-119702 (date of access: 30.08.2025).

21. Olowu O. et al. AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity //Advanced Research and Review. – 2024. – Vol. 21 (2). – pp. 227-237.

22. Badreddine A., Larbi Cherif H. Artificial Intelligence And its applications in E-Commerce //Journal of Private Law. – 2024. – Vol. 2 (1). – pp. 1-15.

23. Alessa H. The role of Artificial Intelligence in Online Dispute Resolution: A brief and critical overview //Information & Communications Technology Law. – 2022. – Vol. 31 (3). – pp. 319-342.

24. Alessa H. The role of Artificial Intelligence in Online Dispute Resolution: A brief and critical overview //Information & Communications Technology Law. – 2022. – Vol. 31 (3). – pp. 319-342.

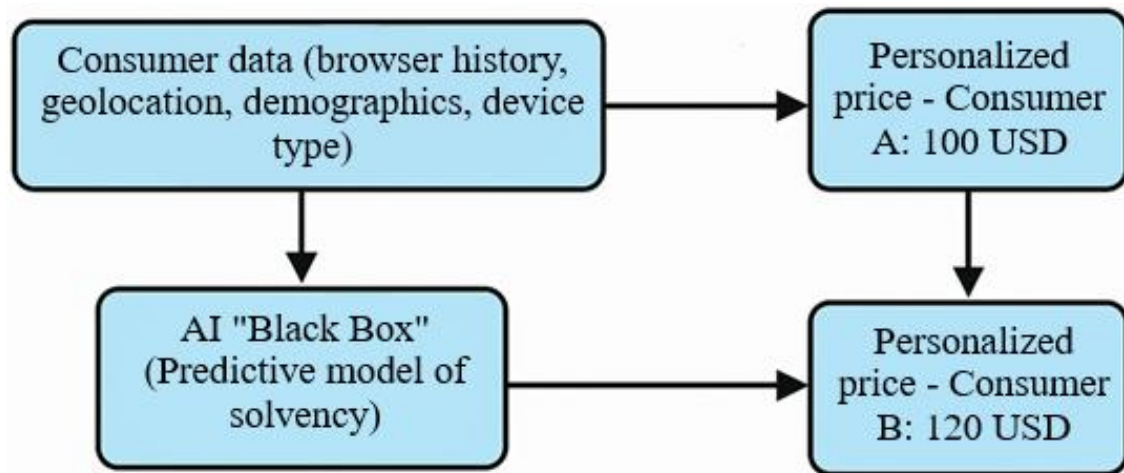*The Am. J. Polit. Sci. Law Criminol. 2025*

14

Figure

Fig. 1. Conceptual diagram of algorithmic price discrimination (compiled by the author based on [9]).
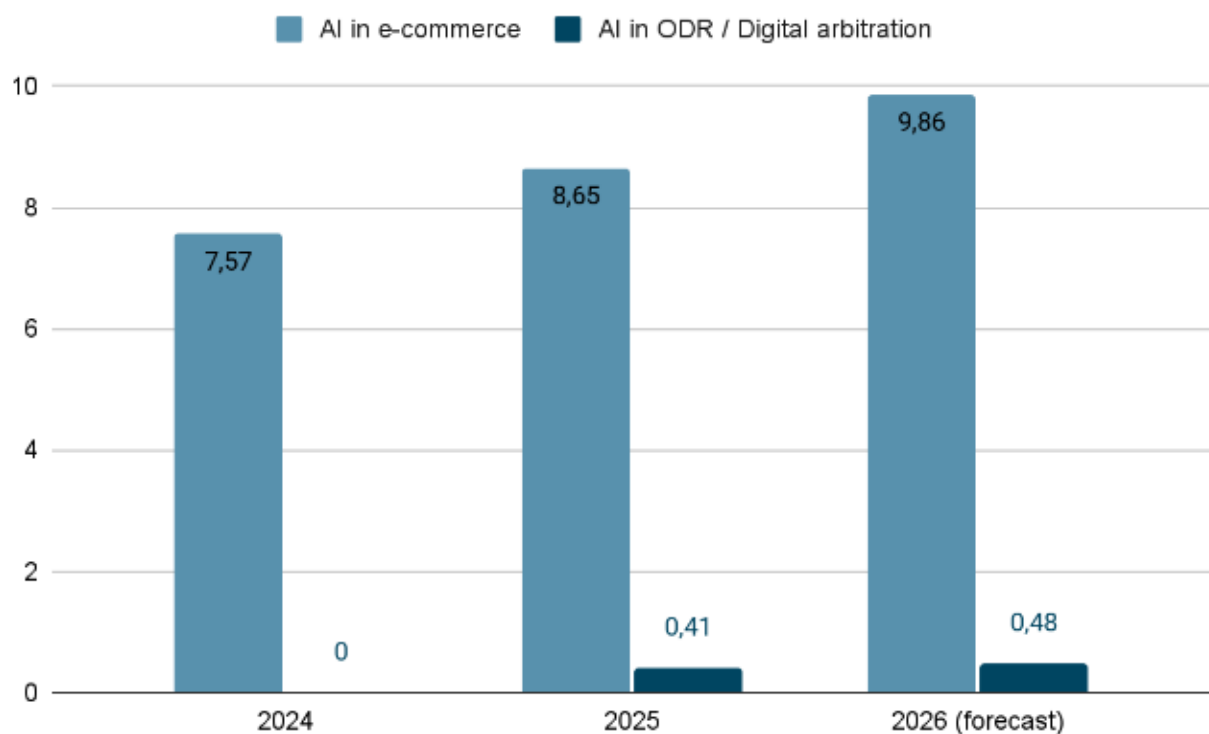

Fig. 2. Forecast for growth of AI markets in e-commerce and online dispute resolution (2024–2026) (compiled by the author based on [1, 7]).