Ljiljana Stanković[1]*
Maja Dimić[2]
Violeta Babić[3]
Lazar Cvijić[4]
Daliborka Jović-Stanković[5]

JEL: F13, L81, O31
DOI: 10.5937/industrija53-63172
UDC: 658:004.8]:339.024
004:007]:004.056

Review Paper

The Significance of Regulating Artificial Intelligence and Cybersecurity for Sustainable Trade

Article history:
Received: 12 December 2025
Sent for revision: 30 December 2025
Received in revised form: 5 February 2026
Accepted: 16 February 2026
Available online: 20 March 2026

***Abstract**: The accelerated digitalization of trade and the growing use of artificial intelligence (AI) offer significant economic benefits but also raise important concerns related to data protection, privacy, and cybersecurity. This paper examines the importance of regulating AI and cybersecurity for the sustainable development of trade, based on the assumption that a stable and coherent regulatory framework is essential for market resilience, consumer trust, and long-term competitiveness. The analysis provides a comparative overview of the regulatory models of the European Union and the Republic of Serbia, focusing on key instruments such as the AI Act, the NIS2 Directive, the GDPR, and relevant national strategies and legislation. The findings show that the EU relies on an integrated approach linking innovation, safety, and consumer rights, while the Serbian framework remains fragmented and in transition. Special attention is devoted to the implications of these regulations for trading companies, business partners, and consumers, as well as to the need for harmonizing national policies with EU standards. The paper concludes that*

[1] University "Union – Nikola Tesla", Faculty of Business Studies and Law, Belgrad, ljiljana.stankovic@fpsp.edu.rs
[2] University "Union – Nikola Tesla", Faculty of Business Studies and Law, Belgrad
[3] Universtity of Niš, Faculty of Agriculture in Kruševac, Serbia
[4] University "Union – Nikola Tesla", Faculty of Business Studies and Law, Belgrad
[5] Game Universum d.o.o., Director and Legal Counsel, Belgrade, Serbia

regulating AI and cybersecurity plays a decisive role in building a secure, transparent, and competitive trade ecosystem in the digital economy.

***Keywords**: artificial intelligence, cybersecurity, digital regulation, European regulatory framework, Serbia, trade, consumer protection.*

Značaj regulisanja veštačke inteligencije i sajber bezbednosti za održivi razvoj trgovine

***Apstrakt**: Ubrzana digitalizacija trgovine i sve intenzivnija primena veštačke inteligencije (AI) donose brojne ekonomske prednosti, ali istovremeno otvaraju važna pitanja u vezi sa zaštitom podataka, privatnošću i sajber bezbednošću. Ovaj rad razmatra značaj regulisanja AI i sajber bezbednosti za održivi razvoj trgovine, polazeći od stava da stabilan i jasno definisan regulatorni okvir predstavlja osnov za tržišnu otpornost, poverenje potrošača i dugoročnu konkurentnost. Analiza obuhvata uporedni prikaz regulatornih modela Evropske unije i Republike Srbije, sa fokusom na ključne instrumente AI Act, NIS2 direktivu i GDPR u poređenju sa relevantnim domaćim zakonima i strategijama u oblasti informacione bezbednosti i razvoja veštačke inteligencije. Rezultati ukazuju da je evropski model zasnovan na integrisanom pristupu koji povezuje inovacije, bezbednost i zaštitu potrošača, dok je u Srbiji regulatorni okvir i dalje fragmentaran i u fazi prilagođavanja. Posebna pažnja posvećena je uticaju ovih propisa na trgovinska preduzeća, njihove partnere i potrošače, kao i potrebi usklađivanja nacionalnih politika sa evropskim standardima. Zaključuje se da regulisanje AI i sajber bezbednosti ima ključnu ulogu u izgradnji bezbednog, transparentnog i konkurentnog trgovinskog ekosistema u digitalnoj ekonomiji.*

***Ključne reči**: veštačka inteligencija, sajber bezbednost, digitalna regulativa, evropski regulatorni okvir, Srbija, trgovina, zaštita potrošača.*

1. Introduction

The digital transformation of the trade sector has brought clear improvements in efficiency, accessibility, and competitiveness, while at the same time opening a number of new challenges related to data protection, privacy, and cybersecurity. Trading companies, especially those operating in complete digital environments, process large volumes of sensitive information every day, including personal and financial data of consumers. This makes them increasingly attractive targets for sophisticated cyberattacks (ENISA, 2023).

Under these conditions, information security can no longer be viewed merely as a technical function. It becomes a strategic priority and an integral part of business resilience. Over the past decade, the European Union has built a coherent regulatory framework that connects technological innovation with the protection of user rights. Instruments such as the GDPR, the NIS2 Directive and the AI Act aim to strengthen the stability of digital markets and reinforce consumer trust (European Commission, 2024a; European Parliament and Council, 2016).

Serbia, as a candidate country for EU membership, is in the long process of aligning its regulatory structure with European standards. Nevertheless, significant institutional and technical challenges remain, especially in the implementation of cybersecurity rules and AI-related regulations (RATEL, 2023; Government of the Republic of Serbia, 2020).

The aim of this paper is to examine the importance of regulating artificial intelligence and cybersecurity for the sustainable development of trade, based on a comparative analysis of EU and national regulatory models. Special attention is given to the implications of these frameworks for trading companies, their business partners and consumers, as well as to the potential for harmonizing national policies with EU standards.

The research is based on an analysis of relevant EU and Serbian legislation, strategies and institutional reports, using a methodological approach that combines legal, economic and technological perspectives on digital transformation (OECD, 2024; WEF, 2023). In this way, the paper positions itself within the field of interdisciplinary research that connects trade, technology and regulation, and highlights the importance of secure and responsible development of the digital economy.

The contribution of the paper lies in an integrated EU - Serbia comparative framework, with a particular focus on the operationalization of “security by design” as a link between regulatory requirements and market competitiveness. Security by design refers to the principle that security and data protection measures are embedded in system architecture from the very beginning, forming an integral part of planning, development and implementation rather than a subsequent or corrective technical measure.

2. Theoretical and Regulatory Framework

2.1. The Need for Integrating Law, Economics and Technology in Modern Trade

Digital transformation has brought significant changes to the structure of market relations and introduced new patterns of market operation within the trade sector. Information technologies are no longer merely a support to business operations but a key factor shaping competitiveness, efficiency and access to consumers. Modern trade is no longer limited by physical space or traditional supply chains. It now operates through complex digital ecosystems that connect all participants within marketing channels, including producers, a range of commercial intermediaries, online stores and platforms, business buyers, financial institutions and consumers (OECD, 2024).

In this environment, the boundaries between the economic, technological and legal dimensions of business activity are increasingly blurred. This creates the need for an integrated model that can simultaneously ensure market efficiency, legal certainty and technological accountability (WEF, 2023). Such an approach enables contemporary, highly digitalized marketing channels to function as a coherent system in which innovation is encouraged while consumers, other market participants, the market itself and the data that sustain it remain protected (European Commission, 2024b).

The integration of law, economics and technology has therefore become a necessary framework for understanding modern trade processes. The economic dimension includes issues of efficiency, costs and competitiveness. The technological dimension defines the capabilities and risks inherent in digital systems. The legal dimension provides regulation that primarily protects consumers, strengthens cybersecurity and prevents the misuse of data (ENISA, 2023).

Regulators and lawmakers must establish a balance between fostering innovation and managing risks so that trading companies can benefit from artificial intelligence and digital technologies without undermining consumer rights or market stability. Since the fields of artificial intelligence and cybersecurity are developing much faster than traditional regulatory frameworks, an integrated approach is becoming an increasingly important tool for managing risks and strengthening trust in the digital economy.

This concept requires cross-sector cooperation among state institutions, the business community, academia and organized consumer groups in order to adapt legal and institutional mechanisms to dynamic market developments (OECD, 2023). Only through such coordination is it possible to ensure that

technological development contributes to sustainable economic growth and stronger consumer protection, rather than deepening digital inequalities.

2.2. The Role of Artificial Intelligence in Modern Trade

Artificial intelligence (AI) has become one of the key technological drivers of transformation in the trade sector, influencing nearly all stages of the value chain, from procurement and logistics to customer interaction and post-sales activities. Trading companies increasingly rely on AI systems to improve operational efficiency, enhance demand forecasting, automate routine tasks and personalize the customer experience (OECD, 2024). The introduction of AI technologies supports better-informed decision making, dynamic pricing and stronger cybersecurity, contributing to a data-driven trade ecosystem capable of quickly responding to market changes (WEF, 2023; The Economist, 2025b).

Table 1. Application of Artificial Intelligence in the Trade Sector

Area of application	Specific activities	Practical examples
Inventory and logistics management	Demand forecasting, procurement and stock optimization, supply chain management, automated warehouses	Walmart uses AI cameras to track inventory levels and predict shortages
Personalization and marketing	Customer data analysis, product recommendations, customer segmentation, dynamic pricing	Amazon uses AI algorithms for product recommendations and personalized offers
Customer experience and support	Chatbots and virtual assistants, sentiment analysis, voice-based shopping	IKEA uses the AI chatbot Billie to provide 24/7 customer support
Price and revenue management	Dynamic pricing, competition monitoring, automated promotions	Amazon adjusts product prices up to two million times per day
Analytics and decision making	Predictive analytics, sentiment analysis, decision-intelligence systems	Carrefour uses AI to analyse consumer behaviour and support sales planning
Retail automation	Self-checkout systems, smart cameras, product recognition	Amazon Go uses AI for item recognition and automated billing
Cybersecurity and risk management	Fraud detection, anomaly analysis, recommendations for protective measures	Fintech platforms use AI to monitor suspicious transactions
Workforce management	Shift planning, productivity analysis, staff training	Tesco uses AI systems for shift scheduling

Source: Author's compilation based on European Commission (2024a), ENISA (2023), OECD (2024) and The Economist (2025b).

Table 1 provides an overview of the main areas in which artificial intelligence is applied in contemporary trade and illustrates how these technologies

simultaneously support business optimization and strengthen consumer protection.

The growing integration of artificial intelligence into trade processes requires the development of a coherent regulatory framework that ensures transparency, accountability and security in data processing and algorithmic decision making (European Commission, 2024a). Regulation must clearly define the limits of automated decisions, establish responsibility for errors and discriminatory outcomes generated by AI, and prescribe mandatory risk assessments in the areas of cybersecurity and personal data protection.

At the same time, ethical principles such as algorithmic explainability, human oversight and the prohibition of discrimination must be incorporated into national legislation and corporate governance frameworks (WEF, 2023; OECD, 2024). In the context of Serbia and comparable developing economies, introducing sector-specific guidelines and certification schemes aligned with the EU Artificial Intelligence Act represents a crucial step toward the safe and responsible use of AI in the trade sector (Government of the Republic of Serbia, 2020; RATEL, 2023).

2.3. The Interconnection Between AI Regulation and Cybersecurity in the Trade Sector

Regulating artificial intelligence and cybersecurity in the trade sector encompasses two areas that are closely related yet conceptually distinct. Cybersecurity refers to the protection of networks, information systems and data from unauthorized access, theft, manipulation or other forms of cyberattacks. This field includes technical, organizational and legal measures that safeguard the integrity, confidentiality and availability of data (ENISA, 2023). At the level of the European Union, cybersecurity regulation is grounded in the NIS2 Directive (2022) and the General Data Protection Regulation (GDPR) (2016/679), while in Serbia the key provisions derive from the Law on Information Security adopted in 2016 and later amended (European Parliament and Council, 2016; Government of the Republic of Serbia, 2025).

AI regulation, by contrast, is focused on the ways in which AI systems operate and on the effects their decisions may have on individuals, markets and consumer rights. The European AI Act (2024) introduces a risk-based classification of AI systems and prescribes specific obligations for high-risk applications, particularly in the fields of financial services, employment, consumer monitoring and digital trade (European Commission, 2024a). This framework establishes standards relating to transparency, human oversight and risk assessment, linking ethical requirements with the conditions for long-term economic sustainability (OECD, 2024; WEF, 2023).

These two regulatory domains are strongly interdependent. Artificial intelligence relies on cybersecurity because AI systems process large volumes of data whose protection is essential for algorithmic reliability and the lawful processing of consumer information. At the same time, modern cybersecurity systems increasingly rely on AI: machine-learning algorithms support earlier detection of anomalies, fraud identification and the prevention of sophisticated attacks (ENISA, 2023). In this way, AI becomes a tool for strengthening digital resilience, while cybersecurity emerges as a fundamental prerequisite for trust in automated decision-making systems.

It follows that AI regulation and cybersecurity form two complementary pillars of digital resilience in the trade sector. While AI regulation provides ethical and legal oversight of algorithms and automated decisions, cybersecurity ensures the technical and systemic protection of digital infrastructure and data. Their integration through a security-by-design approach has become essential for building trust in digital trade, as well as an important reputational factor for companies operating in environments characterized by high technological complexity (European Commission, 2024a; OECD, 2024).

2.4. The Multi-Layered Dimensions of AI Application and Cybersecurity in Trade

The application of artificial intelligence and the provision of cybersecurity in the trade sector have a multi-layered structure and encompass three interconnected levels of responsibility and risk (OECD, 2024; ENISA, 2023).

The first level concerns the internal security and reliability of trading companies themselves, particularly the use of AI technologies within back-office functions such as procurement planning, inventory management, financial analytics and the automation of administrative procedures. At this level, it is essential to ensure the integrity of data and the protection of business information processed by AI systems, as well as to establish clear access-control mechanisms and accountability procedures for employees who oversee automated processes (European Commission, 2024a). Applying the principle of “security by design” enables companies to build digital resilience from the earliest stages of transformation (ENISA, 2023).

The second level relates to relationships and data exchange with business partners across supply chains and marketing channels, including manufacturers, distributors, wholesalers, retailers and providers of logistics, IT and marketing services (OECD, 2024). Integrating AI into these processes creates a need for harmonized cybersecurity standards among partners, greater transparency of algorithms used in shared platforms and contractual

protection of data exchanged along the value chain (ENISA, 2023; WEF, 2023). Risks at this level often arise from uneven levels of protection or technical (in)compatibility between partners' systems, which can result in breaches involving business or personal data (RATEL, 2023).

The third level concerns the interaction between trading systems and consumers, that is, the safety and transparency of using artificial intelligence in direct engagement with end users (European Commission, 2024a; European Parliament and Council, 2016). This level includes systems for offer personalization, customer-behaviour tracking, personal data processing and automated decision-making related to purchasing conditions. In this context, cybersecurity and AI regulation are directly linked to consumer protection, as it is necessary to ensure lawful and fair data processing, prevent manipulation and discrimination, and guarantee consumers' rights to information, consent and human oversight of automated decisions (European Parliament and Council, 2016; WEF, 2023).

All three dimensions internal corporate security, secure collaboration with partners and consumer protection form together a unified framework of digital responsibility in modern trade (OECD, 2024). Because of this multi-layered structure, integrated cybersecurity policies and AI regulation are crucial for building trust in the digital marketplace and for safeguarding the integrity of trade ecosystems (ENISA, 2023; WEF, 2023).

2.5. Security by Design as Reputational Capital

At all levels of artificial intelligence deployment in the trade sector, whether in internal business processes, collaboration with partners or interactions with consumers, the principle of security by design has become one of the defining elements of responsible digital transformation. In a contemporary business environment that increasingly relies on automated systems, algorithmic decision making and digital services, security can no longer be understood solely as a technical matter. It has evolved into a strategic resource that directly shapes market value and stakeholder trust (ENISA, 2023; OECD, 2024).

The essence of the security by design concept lies in embedding the principles of security, privacy and ethical data use into the very foundations of business processes, information systems and algorithms. This means considering security from the earliest conceptual stages, throughout development and implementation, and during everyday use and continuous system oversight (European Commission, 2024a; WEF, 2023). For trading companies, this approach carries several important advantages (The Economist, 2025d). It enables proactive risk management because protection mechanisms are not added as an afterthought but built into every step of system design. It also

facilitates regulatory compliance and supports the effective implementation of frameworks such as the GDPR, the NIS2 Directive and the AI Act, thereby reducing exposure to penalties and reputational harm (European Parliament and Council, 2016; European Parliament and Council, 2022; European Commission, 2024a). Finally, security by design becomes a strategic factor of differentiation because consumers and partners increasingly value digital services that are reliable, transparent and ethically governed. Trust has emerged as one of the most important assets of the digital economy (The Economist, 2025a; WEF, 2023; OECD, 2024).

Introducing this approach in the trade sector means that cybersecurity and data protection are no longer perceived as unavoidable costs but as long-term investments in business reputation and stability (OECD, 2024). Companies that establish strong security standards and ensure that their AI-driven systems are reliable, explainable and accountable build reputational capital that can become a durable competitive advantage (ENISA, 2023). In the digital economy, trust operates as a form of currency, while security stands as one of the fundamental conditions for sustainable business performance (WEF, 2023).

In the context of Serbia and the wider region, the adoption of security by design reflects an important level of institutional and market maturity. Its consistent implementation can strengthen consumer confidence in electronic commerce, enhance cooperation with international partners and accelerate alignment with European standards (RATEL, 2023; Government of the Republic of Serbia, 2020). In this way, security exceeds the boundaries of a mere regulatory requirement and becomes an integral element of business strategy and corporate culture. It connects technical resilience, legal compliance and the broader social responsibility of trading companies. At the same time, this concept provides a theoretical bridge to the following section of the paper, which examines the comparative perspectives of European and national regulatory approaches.

3. Theoretical and Regulatory Framework

The methodological framework of this study is based on a qualitative approach and a review research design aimed at identifying and critically examining existing regulatory, institutional and theoretical models of applying artificial intelligence and cybersecurity in the trade sector. This approach makes it possible to detect key patterns, differences and interconnections between the European and national regulatory frameworks, as well as to assess their impact on the sustainable development of the trade sector (OECD, 2024; ENISA, 2023).

The core of the research consists of a systematic review of the most relevant legal and strategic documents of the European Union. Particular attention is given to acts such as the AI Act (2024), the NIS2 Directive (2022), the Cyber Resilience Act (2023), the General Data Protection Regulation GDPR (2016/679), the Digital Services Act (2022) and the Digital Markets Act (2022). In parallel with these EU regulations, the analysis includes key Serbian legislation, including the Law on Information Security (2016, amended 2025), the Law on Personal Data Protection (2018) and the Artificial Intelligence Development Strategy 2020–2025 (2020) (Government of the Republic of Serbia, 2023; 2018; 2020).

In addition to normative sources, the study incorporates reports and publications from relevant institutions such as ENISA, OECD, the European Commission, RATEL, the Office for IT and eGovernment and the Commissioner for Information of Public Importance and Personal Data Protection. These documents provide further insight into institutional practices and the challenges associated with implementing regulations in the digital environment (RATEL, 2023; European Commission, 2024a; ENISA, 2023; OECD, 2024).

The methodological approach combines comparative and analytical descriptive methods, along with interpretative analysis and an examination of correlations between regulatory models and their economic and institutional effects (WEF, 2023). Special attention is devoted to understanding how AI and cybersecurity regulations influence three key levels of the trade system:

- internal business processes,
- relations with business partners and
- interactions with consumers.

Based on this approach, the study not only offers a review of existing regulatory solutions but also provides a critical assessment of their practical application and developmental potential. In doing so, it contributes to a broader understanding of the role of regulation in shaping a secure, transparent and competitive trade ecosystem within the digital economy (The Economist, 2025b; OECD, 2024).

4. Comparative Analysis and Discussion

4.1. Comparative Analysis of Artificial Intelligence and Cybersecurity Regulation in the EU and Serbia

The regulatory framework of the European Union in the field of artificial intelligence and cybersecurity is widely regarded as the most advanced and coherent model in contemporary international practice. Over the past decade, the EU has developed a broad set of legal instruments designed to strengthen digital resilience, protect personal data and promote the ethical use of technology across economic sectors. Among the most significant are:

- AI Act (2024), the first comprehensive law on artificial intelligence, which introduces a risk-based classification of AI systems and prescribes mandatory requirements for high-risk systems, including standards for data governance, algorithmic transparency and human oversight.
- NIS2 Directive (2022), aimed at reinforcing cybersecurity in key sectors and among digital service providers through obligations related to incident reporting, risk assessment and management level accountability.
- GDPR (2016/679), the central EU framework for personal data protection, which also governs data processing in artificial intelligence systems.
- Cyber Resilience Act (2023), a regulation establishing mandatory security requirements for products with digital components throughout their entire life cycle.
- Digital Services Act (2022) and Digital Markets Act (2022), two instruments that set rules for the responsibilities of digital platforms, algorithmic transparency and user protection (European Commission, 2024a).

In addition to binding regulatory instruments, the European Commission also outlines strategic priorities for the development and governance of artificial intelligence within the Digital Single Market (European Commission, 2024b).

The European model relies on an integrated approach in which cybersecurity, data protection and the regulation of artificial intelligence form a unified and mutually aligned system. This approach is supported by specialised EU level institutions such as ENISA (European Union Agency for Cybersecurity), the EDPB (European Data Protection Board) and the AI Office, a newly established

body responsible for coordinating the implementation of the AI Act and monitoring AI related risks across the Union (ENISA, 2023).

In contrast to the EU, the regulatory framework of the Republic of Serbia is still in a developmental stage and remains relatively fragmented. It is currently built around three principal pillars:

- The Law on Information Security (2016, amended 2025), which is partially aligned with the first NIS Directive but does not yet fully transpose the standards introduced by NIS2. It establishes obligations for public authorities, operators of essential ICT systems and national CERT structures.
- The Law on Personal Data Protection (2018), modelled on the GDPR, though lacking sufficiently detailed provisions on automated decision making and profiling in AI systems (Government of the Republic of Serbia, 2018).
- The Artificial Intelligence Development Strategy of the Republic of Serbia 2020–2025, which outlines strategic objectives for AI development and deployment but does not introduce legally binding rules concerning ethics, accountability or institutional oversight (Government of the Republic of Serbia, 2020).

The Republic of Serbia laid the foundations for AI development by adopting its first Artificial Intelligence Development Strategy for the period 2020–2025. In addition, the Government introduced the Ethical Guidelines for the Development, Implementation and Use of Trustworthy and Responsible Artificial Intelligence (Government of the Republic of Serbia, 2023), marking the first national effort to align ethical principles with practical AI governance. Serbia is also preparing its first Artificial Intelligence Law, for which a multidisciplinary Working Group has been formed to develop a comprehensive regulatory framework. In parallel, a new Artificial Intelligence Development Strategy for the period 2024–2030 is under preparation and is expected to be adopted in the near future.

At the institutional level, Serbia has established the Institute for Artificial Intelligence of Serbia (IVI), which performs research and development functions but does not hold regulatory authority. Supervision of personal data processing is carried out by the Commissioner for Information of Public Importance and Personal Data Protection. Although these institutions contribute to the development of the AI ecosystem, they do not form a unified regulatory architecture capable of overseeing the broader risks and systemic implications of artificial intelligence.

In the domain of cybersecurity, the key institutions include the Office for Information Technologies and eGovernment (Kancelarija za IT i eUpravu), the

Regulatory Agency for Electronic Communications and Postal Services (RATEL) and the National Computer Emergency Response Team (National CERT). Despite some positive developments, this institutional and normative structure does not yet provide a fully coordinated or systematic approach to digital security and the regulation of AI technologies, as confirmed by the most recent reports of the relevant authorities (RATEL, 2023).

Table 2 provides a comparative overview of the principal differences between the European and Serbian regulatory frameworks in the areas of artificial intelligence, cybersecurity and data protection. The table summarizes key points of alignment, institutional distinctions and ongoing reforms that shape the digital security landscape in the EU and Serbia. This overview helps clarify the scope of obligations arising from European standards as well as the challenges faced by the national regulatory system in the harmonization process.

Although Serbia's fundamental principles of data protection and information security are largely aligned with the European model, the existing legislation still does not provide an integrated approach to managing the risks associated with artificial intelligence. The European Union has established a normative structure in which AI governance, cybersecurity and digital services operate as parts of a unified framework of digital resilience. In Serbia, by contrast, these areas remain dispersed across different sectors, which complicates coherent implementation and limits the effectiveness of regulatory oversight.

A key challenge for the national regulatory system will be the consolidation of existing legislation into a coherent architecture of digital security that includes artificial intelligence, personal data protection and cybersecurity (OECD, 2024). Such integration is not only a formal requirement within the EU accession process but also an essential condition for strengthening consumer trust, improving the stability of digital trade and enhancing the competitiveness of domestic companies in the European market (European Commission, 2024a; Government of the Republic of Serbia, 2023).

This process also lays the groundwork for applying the principle of security by design, which connects technological innovation, regulatory accountability and trust as the central pillars of sustainable trade development in the digital economy (WEF, 2023). Without such integration, each of these policy areas operates in isolation, reducing the efficiency of the broader regulatory system and increasing overall exposure to risk.

Table 2. Comparative Overview of AI and Cybersecurity Regulation in the EU and Serbia

Area	European Union (EU)	Republic of Serbia
Regulation of artificial intelligence (AI)	AI Act (2024), risk-based classification of systems, mandatory requirements for high-risk systems including data governance, transparency, human oversight and conformity assessment.	Artificial Intelligence Development Strategy 2020–2025, strategic document without binding legal norms, focus on research and development; Ethical AI Guidelines (2023); Artificial Intelligence Law and new AI Development Strategy 2024–2030 under preparation.
Institutional framework for AI	AI Office (2024), coordination of AI Act implementation; national supervisory authorities in Member States.	Institute for Artificial Intelligence (2021), research institution without regulatory powers.
Cybersecurity (NIS2)	NIS2 Directive (2022), obligations for operators of essential services, management accountability, incident reporting.	Law on Information Security (2016, amended 2025), partially aligned with NIS; limited coverage of the private sector.
Personal data protection	GDPR (2016/679), data protection impact assessments; oversight by EDPB.	Law on Personal Data Protection (2018), no explicit provisions on AI based profiling.
Security of digital products	Cyber Resilience Act (2023), security requirements and mandatory certification for digital products.	No equivalent instrument; partially covered by technical regulations.
Digital platforms and transparency	Digital Services Act and Digital Markets Act (2022), obligations related to algorithmic transparency and user protection.	No dedicated legislation; partially regulated by the Consumer Protection Act and the Electronic Commerce Act.
Supervisory institutions	ENISA, EDPB, AI Office, coordinated system with interconnected mandates.	RATEL, Office for IT and eGovernment, National CERT, Commissioner; fragmented supervisory structure.
Planned reforms	Ongoing regulatory updates, harmonisation of Member States, links with EU green policies.	Planned transposition of the NIS2 Directive, preparation of the national Artificial Intelligence Law, and development of the new AI Development Strategy 2024–2030.

Source: Author's compilation based on EU legislation (European Commission, 2022–2024) and national legislation and documents of the Republic of Serbia (Government of the Republic of Serbia, 2018–2023; RATEL, 2023).

The analysis demonstrates that the development of artificial intelligence and the advancement of cybersecurity in the trade sector are not merely technical issues but above all institutional and regulatory challenges. Establishing a secure, ethical and competitive digital market requires alignment of Serbian legislation with European standards as well as stronger cooperation among institutions responsible for supervising information technologies, data

protection and consumer protection (ENISA, 2023; OECD, 2024). Only through such coordination can a stable and reliable framework be achieved, one that supports the continued growth of digital trade and its capacity to respond to technological and market changes.

4.2. Implications of Artificial Intelligence and Cybersecurity Regulation for the Trade Sector in the EU and Serbia

The regulatory framework governing artificial intelligence and cybersecurity has a strong and multilayered impact on the trade sector, reshaping the way the flow of goods, digital services, and data is planned, organized, and controlled. In the European Union, the establishment of a unified and clearly defined regulatory architecture creates a stable and predictable environment for businesses that rely on AI technologies. The obligations introduced by the AI Act and the NIS2 Directive enable companies to develop innovative digital services such as automated logistics, personalised marketing and advanced risk-management systems, while operating within a high level of legal certainty and institutional support (European Commission, 2024a; ENISA, 2023).

Although this framework increases compliance costs, as businesses must invest in internal security policies, certification processes and data-governance mechanisms, experience across the EU shows that such costs represent a long-term investment. Companies that comply with data-governance and security requirements gain reputational and competitive advantages. In this sense, cybersecurity becomes an investment in market trust and corporate credibility (OECD, 2024; WEF, 2023). Firms that adopt this approach already enjoy additional benefits: they improve transparency in interactions with partners and customers, enhance the efficiency of their logistics, tailor their offers more effectively and strengthen overall operational resilience (Stanković & Cvijić, 2024; Cvijić & Stanković, 2023). Security and innovation thus increasingly function as mutually reinforcing pillars of competitiveness in digital trade (The Economist, 2025c). This link between innovation capacity and market competitiveness is also affirmed in broader analyses of national innovation performance (Stojković et al., 2022). Earlier analyses of structural change in trade and marketing channels similarly emphasise how digital technologies reshape competitive dynamics and the relationships between producers, intermediaries and consumers (Stanković, 2014).

In Serbia, the implications are more complex. Although basic legal mechanisms exist, the absence of an integrated and coordinated regulatory system leads to uneven application of rules in practice (Vlada RS, 2020; RATEL, 2023). Large companies and multinational corporations tend to align with European standards, while small and medium-sized enterprises often lack the technical

knowledge, financial resources and institutional support needed to meet cybersecurity and data-protection requirements. Earlier analyses of structural transformation in the Serbian trade sector confirm these disparities, showing that smaller traders face greater organisational and technological barriers in adopting advanced digital and security standards (Stanković, Babić & Cvijić, 2020). As a result, a gap emerges between regulatory ambition and the real capacities of market actors, slowing digital transformation and reducing the competitiveness of domestic traders.

From an institutional perspective, the EU model promotes continuous cooperation between regulatory authorities and the business sector, whereas in Serbia a predominantly reactive approach persists. Laws exist, but their implementation depends on individual efforts and fragmented initiatives. Insufficient coordination between public institutions, chambers of commerce, professional associations and educational institutions further hinder the development of a competent ecosystem for the safe and responsible application of AI in commerce (ENISA, 2023; OECD, 2024). Strengthening institutional cooperation, especially through advisory mechanisms tailored to the SME sector, will be essential for transitioning to a more proactive regulatory model.

For consumers, the effects of EU regulation are already evident. Citizens have the right to be informed when interacting with an AI system, to understand how their personal data is processed and to challenge automated decisions that affect their interests (European Parliament and Council, 2016; European Commission, 2024a). In Serbia, such mechanisms are still developing. Consumer protection in digital environments remains partly formal, and the quality of protection depends heavily on interpretation of the law and case-by-case enforcement (Commissioner for Information of Public Importance and Personal Data Protection, 2024). Introducing principles such as explainability, transparency and effective human oversight will be crucial for building trust between consumers and AI-enabled commercial systems.

Overall, the adoption of EU standards in the fields of artificial intelligence and cybersecurity has the potential to significantly enhance transparency, trust and competitiveness within Serbia's trade sector. However, this process requires a clear governmental strategy, stronger institutional coordination and dedicated support mechanisms for small and medium-sized traders. The European Union has already outlined a clear direction: integrating innovation and consumer protection through a unified regulatory framework that sustains digital resilience and market equilibrium (European Commission, 2024a; WEF, 2023).

By gradually transposing European standards and strengthening its institutional capacities, Serbia has the opportunity to transform the safe application of artificial intelligence into a source of sustainable competitiveness and growth.

The development of national regulation should not be viewed merely as an administrative task, but as a strategic process that connects legislation, technological progress and consumer trust, the three foundations of a modern trade system in the digital economy.

5. Prospects for the Development of Regulatory Models for Cybersecurity and Artificial Intelligence in the Trade Sector

In the coming decade, the regulation of artificial intelligence and cybersecurity will be one of the key factors shaping competitiveness, trust and the overall sustainability of the digital economy. The rapid evolution of European legislation, together with the growing interdependence between technology, trade and law, requires national systems to develop flexible, adaptive and long-term sustainable regulatory models. Such models must be capable of responding to accelerated technological change, new categories of risk and rising expectations of consumers (European Commission, 2024a; OECD, 2024).

Within the European Union, the next several years will be marked by the full implementation of major digital regulatory instruments. This primarily includes the AI Act, the NIS2 Directive and the Cyber Resilience Act, which together establish a unified framework for the secure, transparent and ethical use of digital technologies across economic sectors (European Parliament and Council, 2016; European Commission, 2024a). Further strengthening of cooperation between regulatory bodies, the private sector and academic institutions is expected, alongside the development of European certification standards for AI and cybersecurity systems (ENISA, 2023). As a result, the trade sector in the EU is entering a phase in which security, ethics and innovation become equally important dimensions of market value. This approach also sets a benchmark for countries aspiring to European integration, confirming that regulation increasingly acts as an instrument of competitiveness rather than a constraint on market development (WEF, 2023; OECD, 2024).

In Serbia, the next policy steps should be directed toward three interrelated areas of development:

1. The transposition of the NIS2 Directive and the preparation of a national law on artificial intelligence, which would clearly define risks, obligations and security standards for trading companies.
2. Strengthening institutional coordination between RATEL, the Office for IT and eGovernment, the Commissioner for Information of Public

Importance and Personal Data Protection, and the Ministry of Trade, with the aim of establishing a coherent national system of digital resilience.

3. Targeted support for small and medium-sized trading enterprises through training programmes, certification mechanisms and financial incentives for the implementation of AI and cybersecurity solutions (Government of the Republic of Serbia, 2023; RATEL, 2023).

In the coming period, particular importance will be placed on the introduction of standardised security protocols across supply chains, as well as the establishment of a national register of AI systems and certification schemes based on transparency and accountability. These measures will enable Serbian trading companies to operate in alignment with EU requirements, facilitating access to the single market and strengthening their competitive position (European Commission, 2024a; ENISA, 2023).

From a long-term perspective, regulatory development should move toward the creation of a model of sustainable digital trade. In such a system, innovation, security and trust operate in mutual balance (WEF, 2023; OECD, 2024). Technological progress would be assessed not only through economic performance, but also through the level of user protection, market integrity and the quality of ethical standards embedded in digital decision making. For Serbia, this implies building a regulatory architecture that connects legislation, technological infrastructure and consumer trust into a coherent and functional framework. This represents the foundation for the country's deeper integration into the European digital space and for strengthening the resilience of its trade sector in the years ahead.

6. Conclusions

The development of artificial intelligence and the rapid digitalisation of business operations are fundamentally transforming the structure and dynamics of the modern trade sector. The use of AI technologies brings significant benefits in terms of efficiency, advanced analytics and the personalisation of market activities, but it also raises important questions related to data protection, privacy and cybersecurity. In this context, building a stable and coherent regulatory framework that balances innovation and security becomes a necessary precondition for the sustainable development of trade.

AI systems must be grounded in the principles of explainability, transparency and accountability, while cybersecurity must ensure a reliable digital infrastructure, the protection of business and personal data and resilience to emerging threats. In recent years, the European Union has developed a

consistent model of digital regulation that links several key areas, including artificial intelligence through the AI Act, cybersecurity through the NIS2 Directive, data protection through the GDPR and the security of digital products through the Cyber Resilience Act. This integrated approach creates a predictable regulatory environment that encourages innovation and at the same time protects consumers, market competition and trust in digital services.

Compared with this model, Serbia has made certain progress through the adoption of the Law on Information Security and the Law on Personal Data Protection, but it still lacks a unified system that brings together AI regulation and cybersecurity into a functional whole. Existing rules remain fragmented, sectorally divided and largely reactive, which hinders the consistent application of security and ethical standards in the trade sector.

For trade, as one of the most digitalised branches of the economy, these differences have substantial practical implications. In the European Union, a unified regulatory framework enables companies to develop innovative digital services with clearly defined obligations and oversight mechanisms. In Serbia, however, the implementation of regulations often depends on the resources and organisational capacities of individual companies, with small and medium-sized enterprises facing particular challenges due to limited technical support and financial means. Introducing integrated policies, sector-specific guidelines and national legislation aligned with European standards is therefore crucial for modernising trade, strengthening consumer trust and improving the competitiveness of domestic companies on international markets.

The concept of security by design is increasingly recognized as a central principle of the new regulatory model. It requires that security, transparency and ethics are embedded into every stage of the development and use of digital systems, rather than added as an afterthought. Trading companies that adopt this approach not only reduce the risk of incidents and regulatory sanctions, but also strengthen their reputation, build consumer trust and become preferred partners in international supply chains. In the digital economy, security becomes a market value and trust a key currency of sustainable business.

In conclusion, aligning with European standards in the fields of artificial intelligence and cybersecurity should not be viewed merely as a requirement of EU integration, but as a strategic development instrument that enables Serbia to build a secure, transparent and competitive trade environment. Integrating European regulatory models into the national framework, together with stronger institutional cooperation and targeted support for small and medium-sized trading companies, will create the foundations for long-term growth of the digital economy. In this way, the core aspiration of modern trade is achieved: ensuring

that innovation, technology and trust function as mutually aligned pillars of market development in the twenty-first century.

References

Cvijić, L., & Stanković, Lj. (2023). The role of artificial intelligence in the business of trading companies. In LEMiMA 2023 – Proceedings (Vol. 1, pp. 129–132). ISBN 978-86-6102-124-4.

ENISA – European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023. Athens: ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Commission. (2022a). Digital Services Act (Regulation (EU) 2022/2065). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

European Commission. (2022b). Digital Markets Act (Regulation (EU) 2022/1925). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/1925/oj

European Commission. (2024a). Artificial Intelligence Act (Regulation (EU) 2024/1689). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/

European Commission. (2024b). Artificial intelligence in the EU: Priorities for the Digital Single Market. Brussels: European Commission. https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/

European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Government of the Republic of Serbia. (2018). Law on Personal Data Protection. Official Gazette of the Republic of Serbia, No. 87/2018.

Government of the Republic of Serbia. (2020). Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020–2025. Belgrade: Government of the Republic of Serbia. https://www.srbija.gov.rs/tekst/en/149169/strategy-for-the-development-of-artificial-intelligence-in-the-republic-of-serbia-for-the-period-2020-2025.php

Government of the Republic of Serbia. (2023). Ethical Guidelines for the Development, Implementation and Use of Trustworthy and Responsible Artificial Intelligence. Belgrade: Government of the Republic of Serbia.
Government of the Republic of Serbia. (2025). Law on Information Security (amended). Official Gazette of the Republic of Serbia, No. 6/2016, 94/2017, 77/2019 and 91/2025.
Organisation for Economic Co-operation and Development. (2024). OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier. Paris: OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/oecd-digital-economy-outlook-2024-volume-1_d30a04c9/a1689dc5-en.pdf
Regulatory Agency for Electronic Communications and Postal Services (RATEL). (2023). Izveštaj o bezbednosti IKT sistema u Republici Srbiji. Belgrade: RATEL. https://www.ratel.rs
Stanković, Lj. (2014). The Trade Revolution: New Power Relations in Marketing Channels. Belgrade: Čigoja štampa.
Stanković, Lj., Babić, V., & Cvijić, L. (2021). Development of electronic commerce and structural changes in the market. In B. Tešanović (Ed.), Structural Changes and Development (pp. 108–128). Belgrade: Faculty of Business Studies and Law, Union–Nikola Tesla University.
Stanković, Lj., & Cvijić, L. (2024). The importance of developing the field of information security for the market and for the trade of products and services, with reference to the Republic of Serbia. Godišnjak FITI, 2024, 175–194.
Stojković, H. S., Kastratović, E., & Stanković, Lj. (2022). Innovation as a way of increasing the competitiveness of the economy. Trendovi u poslovanju, 19(1), 18–25.
The Economist. (2025a, April 12). *The economics of superintelligence.* The Economist. https://www.economist.com
The Economist. (2025b, April 27). *What if AI made the world's economic growth explode?* The Economist. https://www.economist.com
The Economist. (2025c, July 23). *The dark horse of AI labs.* The Economist. https://www.economist.com
The Economist. (2025d, July 24). *AI labs' all-or-nothing race leaves no time to fuss about safety.* The Economist. https://www.economist.com
World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Geneva: World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/