

LEGAL CONFLICTS IN THE DIGITAL ECONOMY: THE UKRAINIAN AND EUROPEAN EXPERIENCE

Ihor Kovbas¹, Mykola Shkriblyak², Veronika Horielova³

Abstract. This article examines the ethical and legal issues arising in the digital economy. These conflicts are conceptualised as contradictions between innovative technological practices, ethical norms and applicable legislation. Three key types of conflict are identified: those relating to privacy and data monetisation, algorithmic autonomy and accountability, and digital security and fundamental rights. Particular emphasis is placed on the wartime context in Ukraine, which presents unique challenges for digital transformation and legal regulation. *Methodology.* The research methodology employed is a synthesis of the comparative legal method and a Law and Economics approach. The comparative legal method is employed to compare the regulatory instruments of the European Union (GDPR, AI Act, DSA, DMA) with those of Ukraine (the Laws of Ukraine 'On Personal Data Protection', 'On Virtual Assets', 'On Media', and 'On Electronic Communications'). The empirical basis of the study comprises reports by the European Commission (Digital Economy and Society Index, DESI), Eurostat statistical data on the digital transformation of EU Member States, and analytical materials published by the OECD (Digital Economy Outlook) and the World Bank (Digital Development Report). The Law and Economics analysis is employed to evaluate the impact of legal conflicts on the investment climate, transaction costs and innovation activity. *Results.* The study demonstrates that the development of the digital economy in Ukraine and the European Union is determined not only by the pace of digital technology adoption, but also by the quality of the institutional environment in which digital markets operate. The European model is distinguished by the establishment of common rules governing data flows, the utilisation of artificial intelligence, and the operation of digital platforms. This contributes to a reduction in regulatory uncertainty for businesses and the creation of conditions conducive to long-term investment in digital technologies. Ukraine continues to face an institutional and technological gap with the EU, as evidenced by uneven levels of business digitalisation, limited investment capacity among some businesses in digital infrastructure, and heightened risks associated with the use of data and artificial intelligence technologies. At the same time, a lack of clear rules governing the digital economy could lead to higher transaction costs for businesses, reduce investment activity and make it more difficult for Ukrainian companies to access the European digital market. The study establishes that digital regulatory conflicts have not only legal but also direct economic effects: they affect regulatory compliance costs, the level of market competition, access to digital services, consumer trust, and the ability of businesses to scale digital business models. In this context, the harmonisation of Ukraine's digital environment with European approaches may be regarded as one of the factors reducing institutional barriers to digital investment and deepening Ukraine's economic integration with the EU. *Practical Implications.* The practical value of the findings lies in their potential application to shaping Ukraine's economic policy on digital transformation, aimed not merely at regulatory adaptation but, above all, at creating conditions to increase enterprise productivity, attract investment, and expand the participation of Ukrainian firms in European digital markets. Priority areas include reducing regulatory and transaction costs for digital businesses; establishing rules for data flows and AI deployment that align with the European market; promoting

Received on: June 10, 2026 **Accepted on:** August 25, 2026 **Published on:** October 14, 2026

¹ Yuriy Fedkovych Chernivtsi National University, Ukraine (*corresponding author*)

E-mail: ig.kovbas@chnu.edu.ua

ORCID: <https://orcid.org/0000-0001-7039-1586>

² Yuriy Fedkovych Chernivtsi National University, Ukraine

E-mail: m.shkriblyak@chnu.edu.ua

ORCID: <https://orcid.org/0000-0002-6036-5242>

³ V.I. Vernadsky Taurida National University, Ukraine

E-mail: gorielova.veronika@tnu.edu.ua

ORCID: <https://orcid.org/0000-0001-6536-2422>

Web of Science ResearcherID: <http://www.researcherid.com/rid/ABB-9463-2022>



This is an Open Access article, distributed under the terms
of the Creative Commons Attribution CC BY 4.0

the digitalisation of small and medium-sized enterprises; developing digital infrastructure; and encouraging competition in digital markets. The implementation of these measures takes on additional economic significance under martial law, as digital technologies can ensure business continuity, reduce the costs of coordinating economic processes and boost enterprise resilience to external shocks. Therefore, the effectiveness of harmonisation with European digital regulations should be assessed not only by the number of provisions implemented, but also by their impact on investment activity, productivity, competitiveness and the resilience of Ukraine's digital economy. *Value / Originality.* The scientific novelty of the study lies in its identification of the economic consequences of regulatory and ethico-legal conflicts arising during the digital transformation of Ukraine's economy and its integration into the European digital space. The proposed typology of key conflicts enables the systematisation of factors that generate regulatory uncertainty, increase transaction costs, and affect investment activity and the competitiveness of digital economy enterprises. The developed cyclical model of conflict evolution is intended as a tool for identifying the interrelationship between technological change, regulatory adaptation, economic costs, and institutional responses. Its application may prove useful in assessing the digital resilience of the economy, underpinning public policy on digital transformation, and setting priorities for Ukraine's economic integration into the European digital market amid wartime conditions and post-conflict recovery.

Keywords: legal conflicts, digital economy, economic regulation, digital governance, institutional development, digital markets.

JEL Classification: K20, K24, K38, O31, O33

1. Introduction

The rapid development of digital technologies and the digital economy is significantly transforming social relations and bringing the safeguarding of digital human rights to the fore. While the widespread adoption of AI, digital platforms and electronic services contributes to economic growth, it also creates new risks to the exercise and protection of human rights (Kapuliak et al., 2026). The pace of digitalisation far exceeds the capacity of legal systems to adapt to new challenges. This has led to the emergence of 'ethico-legal conflicts' in the digital economy – contradictions between innovative technological practices, ethical norms, and applicable legislation.

The legal regulation of the digital economy has been a key area of study in European scholarship. Considerable attention has been devoted to analysing the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), the Digital Services Act (DSA) and the Digital Markets Act (DMA) (Borovyk et al., 2026; Tytska et al., 2026). Researchers have also addressed the issue of digital inequality and the concentration of innovative resources within start-up ecosystems (Menshikov et al., 2026). At the same time, the vast majority of these studies examine digital regulation within the context of stable, peacetime economies. Despite the substantial body of research on digital regulation, the ethical and legal conflicts that arise in the digital economy under martial law, and their impact on state economic development, remain insufficiently explored.

Amid widespread war, Ukraine's digital transformation has gained distinctive momentum.

The state is actively developing digital services (such as 'Diia'), digital identification systems, public registries and cybersecurity measures. However, martial law creates unique conflicts in Ukraine, including tensions between privacy and national security, the military application of AI, and monitoring of the information space. It is precisely this context that gives the study its potential scientific originality, as most European publications fail to address wartime challenges.

The study aims to identify key ethico-legal conflicts in the digital economy and compare the approaches taken by the EU and Ukraine to address them. It will also propose ways to align Ukrainian legislation with European standards.

2. Theoretical and Economic-Legal Framework

2.1. Conceptual Approaches to Understanding Ethico-Legal Conflicts in the Digital Economy

Ethico-legal conflicts in the digital economy are a natural consequence of the rapid development of digital technologies, the globalisation of information processes, and the transformation of traditional economic relations. The evolving nature of the digital environment gives rise to circumstances in which prevailing legal and regulatory frameworks may not always be sufficiently responsive to novel technological challenges. Concurrently, the economic rationale for implementing digital innovations may encounter discord with fundamental ethical principles and human rights. In such circumstances, the examination of the interrelationship between law, ethics, and technology, as well as the search for effective mechanisms to

resolve conflicts arising within the digital economy of Ukraine and the European space, assumes paramount importance.

The Law and Economics approach, as pioneered by Richard Posner (Posner, 2014), facilitates the evaluation of legal rules in terms of their impact on economic efficiency. The primary advantage of this approach lies in its ability to quantitatively assess regulatory impacts on transaction costs and the investment climate. Nevertheless, its primary constraint is that it frequently neglects to acknowledge fundamental human rights as an inherent value that cannot be diminished to economic indicators.

Important conceptual contributions come from Nick Srnicek's theory of platform capitalism (Srnicek, 2016) and Shoshana Zuboff's concept of surveillance capitalism (Zuboff, 2019). In their work, these scholars explain how digital platforms have emerged as new 'economic infrastructures' and examine how personal data have become 'objects of commercialisation'. As researchers have observed, it is precisely these processes that lay the groundwork for ethico-legal conflicts (Menshikov et al., 2026). However, these theories focus predominantly on economic aspects, leaving legal protection mechanisms largely overlooked. It is evident that none of these approaches, when considered in isolation, is sufficient to account for the full complexity of ethico-legal conflicts in the digital economy. Whilst the Law and Economics paradigm furnishes instruments for economic evaluation, it does not encompass the value-based aspect of human rights. Similarly, theories of platform capitalism reveal the nature of digital markets but do not propose legal safeguards. Therefore, this study takes an integrated approach, combining economic analysis of law with the concept of digital human rights, and considers the wartime context of Ukraine.

The General Data Protection Regulation (GDPR) is a key piece of legislation in the field of European digital law. Of particular relevance to economic activity is the fact that it establishes common rules for processing personal data (European Parliament & Council, 2016). In the economic sphere, the introduction of such rules provides digital market participants with legal certainty and establishes a level playing field for conducting business within the EU. Researchers have noted that the GDPR has introduced a new regulatory model (Kapuliak et al., 2026). At the same time, the practical application of the GDPR has revealed a number of conflicts. Notably, in the Schrems II case (2020), the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield mechanism for data transfers to the United States. This created legal uncertainty for the many companies involved in transatlantic data transfers. From a law and economics perspective, legal uncertainty increases transaction costs for businesses. They are forced to

review data transfer agreements, implement additional compliance mechanisms, conduct legal audits and adapt their internal procedures. Therefore, regulatory requirements directly impact the cost structure of businesses and the conditions in which digital markets operate.

In the context of European integration, the harmonisation of personal data protection legislation with the GDPR is particularly relevant for Ukraine. The current Ukrainian law on personal data protection (The Law of Ukraine "On Personal Data Protection" of June 14, 2025, No. 2297-VI) does not align with contemporary European standards, particularly with regard to the powers of the regulator, the scale of fines and the mechanisms for protecting the rights of data subjects. Failure to fully align with the GDPR imposes additional costs on Ukrainian companies operating with European partners, hinders cross-border data flows and undermines the competitiveness of Ukrainian digital businesses in the EU market.

In 2024, the European Union adopted the Artificial Intelligence Act, hereafter referred to as the 'AI Act'. This comprehensive legislative instrument is the first of its kind to establish common rules for the development, deployment and use of artificial intelligence systems. Its economic significance lies in establishing legal constraints and creating a predictable regulatory environment for businesses, investors and developers of digital technologies. The AI Act introduces a risk-based approach, classifying AI systems according to their potential risk level, ranging from 'unacceptable' to 'minimal'. This approach imposes differentiated requirements on economic operators (European Parliament & Council, 2024). This regulatory model directly impacts economic processes by determining compliance costs, market entry conditions for innovative products, investment risk levels, and enterprise competitiveness. At the same time, establishing common rules could reduce legal uncertainty and boost confidence in AI technologies, creating the conditions for their wider adoption in manufacturing, finance, services and public administration. Consequently, the AI Act should be viewed not only as a means of technological regulation, but also as an economic mechanism that shapes the new rules of competition and risk allocation in the digital economy.

The academic debate surrounding the AI Act centres on a number of key issues. Firstly, there is the question of liability for harm caused by AI systems. Existing legislation fails to take into account the unique nature of algorithmic decision-making, particularly in cases where it is impossible to identify the specific individual whose actions caused the harm (Tytska et al., 2026). Such uncertainty translates into heightened regulatory risk for the digital economy. In the absence of clear liability rules, companies must account for additional legal risks when developing and commercialising

artificial intelligence systems. This can hinder innovation and increase the cost of entering the market for new products. Secondly, there is the issue of algorithmic transparency, particularly with regard to credit scoring, recommendation systems and automated decision-making processes. Enhancing transparency fosters trust among users and investors, and is an essential prerequisite for developing digital markets and scaling innovation.

It is important to note that Ukraine currently lacks dedicated AI regulation. The Concept for the Development of Artificial Intelligence in Ukraine, which was approved by an order of the Cabinet of Ministers of Ukraine in 2020, does not have the force of law. The establishment of specific legislation pertaining to AI remains in its infancy. The absence of comprehensive regulation engenders regulatory uncertainty for businesses, dampens investment in high-tech projects, and restricts the capacity of Ukrainian companies to participate in joint digital projects with EU Member States.

The digital transformation of the economy has engendered novel imperatives for the protection of human rights in the digital environment, exerting a direct influence on the conditions under which digital markets operate. In the academic literature, digital rights are regarded either as a potentially new generation of human rights or as an adaptation of traditional rights to technologically mediated economic and social relations (Kapuliak et al., 2026). Among the rights of greatest relevance to the digital economy are the right to access digital infrastructure and the internet, personal data protection, digital identity, freedom of expression in the digital environment, the right to non-discrimination, and the right to the erasure of personal data (the 'right to be forgotten'). Their realisation has socio-legal and economic significance. The level of digital rights protection determines consumer trust in online services, the willingness of economic operators to adopt digital technologies and the scale of risks associated with data processing. In this context, the European model – shaped in particular by the provisions of the GDPR, the Charter of Fundamental Rights of the European Union, and other digital regulatory instruments – creates institutional conditions that make digital markets more predictable. From an economic perspective, the effective protection of digital rights is a vital pillar of the digital economy. High levels of protection for personal data and digital identities increase consumer trust in e-commerce, digital financial services and public online services. This, in turn, fuels digital economic activity, drives the expansion of e-commerce and reduces transaction costs associated with information asymmetry. However, stricter digital rights protection requirements may increase compliance, cybersecurity, and data management costs for businesses. This

highlights the importance of balancing human rights protection with regulatory burden and fostering digital innovation.

3. Materials and Methods

The study employs a combination of the comparative legal method and law and economics analysis. The comparative legal method is used to compare European Union legal instruments, such as the GDPR, AI Act, DSA and DMA, with Ukrainian legislation. The Law and Economics analysis assesses the impact of legal conflicts on the investment climate, transaction costs and innovation activity. The analysis covers the following EU legislative instruments: the GDPR, the AI Act, the DSA and the DMA. It also covers the following Ukrainian laws: 'On Personal Data Protection', 'On Virtual Assets', 'On Media' and 'On Electronic Communications'.

The empirical basis of the study comprises European Commission reports (DESI), Eurostat statistical data, and analytical materials published by the OECD and the World Bank. The theoretical foundation of the article consists of contemporary scholarly works addressing the digital economy, digital law, and the economic analysis of law. In order to analyse the Ukrainian context, the study relies on data regarding the operation of the 'Diia' digital services, the digital identification system, public registries, and cybersecurity measures implemented under martial law. The data presented herein have been obtained from publicly available reports issued by government authorities and international organisations.

The comparative analysis was guided by the following criteria: the level of protection of personal data, regulation of artificial intelligence systems, liability mechanisms for digital platforms, instruments for ensuring digital security and the extent to which national legislation is harmonised with EU law. The assessment was conducted through a qualitative analysis of legislative instruments and a synthesis of statistical indicators of digital transformation.

A methodological limitation of the study stems from the restricted availability of comprehensive statistical data for the period of martial law (2022–2024), which necessitates the reliance on expert assessments rather than direct statistical observations.

4. Results and Discussion

This study proposes the identification of three key types of ethico-legal conflicts in the digital economy. This proposal is based on an analysis of the academic literature and legislative instruments. The proposed typology encompasses the primary domains of interaction between the state, businesses, and citizens in the digital economy, reflecting the most prevalent

conflicts between economic efficiency, technological development, and human rights protection. The first conflict concerns the commercialisation of data and regulatory compliance. While the GDPR establishes high standards for the protection of personal data, the business models of digital platforms are based on the collection, processing and commercialisation of such data (Kapuliak et al., 2026). The interaction between these two factors creates an economic conflict between maximising the commercial value of data and the costs of complying with regulatory requirements. This directly affects the cost structure of digital businesses.

The second conflict revolves around algorithmic autonomy and the economic allocation of risks in decision-making processes. The integration of artificial intelligence systems in credit scoring, recommendation systems, automated underwriting, and other business processes is effecting a transformation of conventional mechanisms for information assessment and economic decision-making. While the algorithmic processing of large volumes of data can reduce decision-making costs, accelerate customer service and enhance the scalability of business models, it can also create new forms of economic risk. Errors or systematic biases in algorithms may result in the misallocation of credit resources, loss of customers, financial losses and reduced trust in digital services. Another source of uncertainty lies in the difficulty of allocating economic consequences among AI developers, digital platform owners, and other participants in the digital product value chain (Tytska et al., 2026). Consequently, the issue not only concerns legal liability, but also the economic allocation of the risks and costs associated with using autonomous algorithmic systems. This emphasises the importance of regulatory and governance mechanisms that can preserve the economic advantages of automation while minimising the costs resulting from algorithmic errors and a lack of transparency in decision-making processes.

The third issue relates to the interdependence between digital security and the economic efficiency of the digital environment. During martial law, the increasing use of digital identification systems, cybersecurity measures and automated data exchange is essential for maintaining economic processes and enabling digital business models to function. At the same time, excessive or poorly coordinated control mechanisms can increase transaction costs for businesses, complicate access to digital services and reduce the economic incentive to use them. Conversely, insufficient digital security increases the likelihood of cyber incidents, financial losses, operational disruption and business recovery costs. Therefore, digital security is an economic resource because its level directly affects consumer and business trust in digital services, investment activity and the resilience of digital markets.

The proposed typology demonstrates that each type of ethico-legal conflict generates distinct economic costs and affects the functioning of digital markets.

Notably, ethico-legal conflicts in the digital economy are not static; they emerge and transform amid continuous technological and institutional dynamics. An analysis of theoretical approaches has led to the development of a cyclical model that illustrates the sequence through which such conflicts emerge and their impact on economic processes. The first stage is technological innovation. The advent of new technologies – including artificial intelligence, big data, and blockchain – expands opportunities for economic activity, creates new business models, and offers potential for increased productivity. The second stage involves an ethical conflict, which occurs when the deployment of a new technology conflicts with established societal perceptions of privacy, fairness, non-discrimination and acceptable data usage. The third stage is legal uncertainty, which arises when existing regulatory mechanisms fail to keep pace with technological changes, or when they are applied inconsistently. This directly affects the economic behaviour of market participants. The fourth stage comprises economic consequences, including increased transaction costs, heightened risks for investors and businesses, reduced investment activity and slower innovation commercialisation. The fifth stage is regulatory intervention, whereby the state adapts or introduces regulatory mechanisms with the aim of reducing uncertainty and creating more predictable conditions for economic activity. While effective regulatory intervention can mitigate risks and transaction costs, further technological development can create new economic opportunities while simultaneously generating new ethical and regulatory challenges. This triggers the next cycle. Thus, the proposed model not only demonstrates the sequence through which ethico-legal conflicts develop, but also the mechanism by which these conflicts result in economic consequences and subsequent institutional adaptation. Figure 1 presents the proposed cyclical model.

The proposed cyclical model illustrates the recurring nature of conflicts within the digital economy. These conflicts arise whenever technological development outpaces legal regulation. It is essential to understand this cyclical nature in order to shape effective regulatory policies that reconcile the protection of human rights with the need to support innovation.

From an economic analysis of law perspective, each new cycle of conflict is accompanied by additional transaction costs. These costs are at their highest during periods of legal uncertainty, when economic operators are unable to reliably assess regulatory risks. Following legislative adaptation, however, the level of uncertainty decreases, creating a more predictable environment for investment and the adoption of digital innovations.

Table 1

Typology of Ethico-Legal Conflicts in the Digital Economy

Type of conflict	Nature of the conflict	Manifestation in the EU	Manifestation in Ukraine	Key economic consequences	Primary economic effect
Privacy vs data monetisation	Personal data protection vs commercialisation	GDPR and the practice of the European Data Protection Board	Law of Ukraine “On Personal Data Protection” and draft legislation aimed at harmonisation with the GDPR	High compliance costs, capital outflow	Surge in compliance and transaction costs
Algorithmic autonomy vs liability	AI-based decisions vs the inability to determine accountability	EU Artificial Intelligence Act (AI Act)	Fragmentary regulation and draft legislation aimed at alignment with the AI Act	Legal uncertainty, stifled innovation	Heightened investment and regulatory risk
Digital security vs fundamental rights	State access to data vs the right to privacy	Robust legal framework (GDPR, ePrivacy Directive)	Martial law creates unique operational conditions	Compromised trust in digital services	Erosion of trust and digital economic activity

Source: compiled by the authors based on Borovyk et al. (2026), Kapuliak et al. (2026), Menshikov et al. (2026), and Tytska et al. (2026).

The findings partially support the economic analysis of law (Posner, 2014), which assumes that legal uncertainty increases transaction costs. In Ukraine, however, martial law exacerbates this uncertainty further through security-related restrictions, creating an additional layer of regulatory risk that is not considered in classical law and economics literature.

The theory of platform capitalism (Srnicsek, 2016) explains the first conflict, namely the tension between privacy and the monetisation of data. However, the findings also show that this conflict is intensified by the need for state monitoring of the information environment under martial law. This aspect is unaddressed by the theory of platform capitalism, which is inherently oriented towards peacetime conditions.

The concept of surveillance capitalism (Zuboff, 2019) draws attention to the risks associated with the concentration of informational power in the hands of large digital corporations, which gain economic advantages through the large-scale collection, analysis, and commercial use of personal data. The present study extends this concept by demonstrating that, under martial law, analogous risks may also arise from the state, which gains expanded access to personal data under the guise of ensuring national security. This has the effect of intensifying the conflict between digital security and the right to privacy, thereby underscoring the need for independent oversight regarding the use of personal data by both public authorities and private platforms.

In order to substantiate the economic consequences of ethico-legal conflicts, it is necessary to examine data from international organisations. The data indicate a significant discrepancy between Ukraine and the EU average, which creates additional barriers to legislative harmonisation. A particular gap is evident in basic digital literacy: according to Eurostat, 56.56% of the EU population aged 16 to 74 possess at least basic

digital skills. In contrast, this figure is lower in Ukraine, suggesting a shortage of human capital (Eurostat, 2024a). Similarly, data on the frequency of internet use shows a similar trend. In 2024, 88.3% of the EU population used the internet daily (Eurostat, 2024a), compared to 78% of Ukrainian citizens, with 10% not

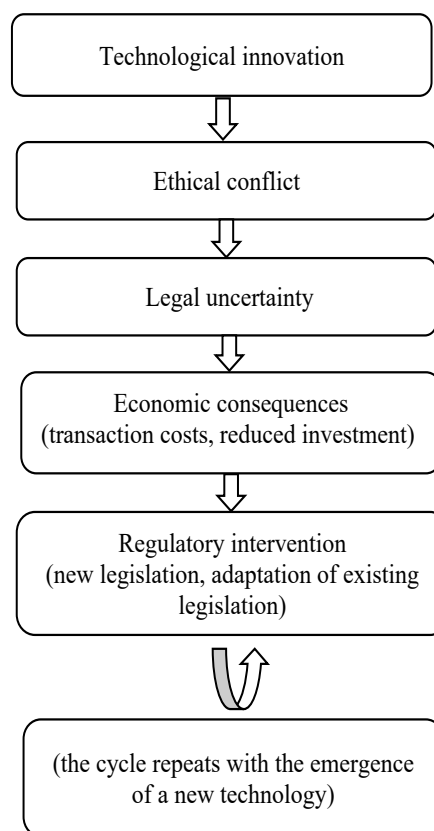


Figure 1. Cycle of Formation and Resolution of Ethico-Legal Conflicts in the Digital Economy

Note. The arrows illustrate the cyclical nature of the emergence of new regulatory conflicts following the introduction of legal changes.

Source: developed by the authors

using it at all (UNDP, 2024). Furthermore, business integration into the digital economy remains critically low. In 2024, just 38.2% of Ukrainian businesses had a corporate website, compared to 78.3% in the EU (Eurostat, 2024b). This reflects the low level of digital adoption among small and medium-sized enterprises (SMEs). In addition, insufficient funding for innovation remains a challenge. Although Ukraine recorded the highest gross domestic expenditure on research and development (R&D) among the Eastern Partnership countries in 2023, at 0.32% of GDP, this figure is still far below the EU average of 2.26% (Eurostat, 2024b).

Global trends likewise confirm the growing importance of digital innovation and artificial intelligence for economic development. According to Dealroom, global venture funding for start-ups totalled 330 billion USD in 2024, marking a 6% increase on the previous year. Notably, investment in companies focused on artificial intelligence reached a record 110 billion USD, marking a 62% year-on-year increase, while investment in other technology sectors declined by 9%. This indicates a shift in investment towards digital technologies and AI, highlighting the urgent need for modern regulatory frameworks for the digital economy and AI systems (Dealroom, 2024). These data suggest that contemporary interstate competition is increasingly focused on attracting investment in high-technology sectors. In such circumstances, the quality of digital regulation becomes a key economic factor in international competitiveness. A predictable legal environment mitigates regulatory risk for investors, whereas legal uncertainty can severely hinder venture capital inflows, even in regions with substantial human capital potential.

Table 2

Digital Transformation Indicators: EU and Ukraine

Indicator	EU (average)	Ukraine
Daily internet use (% of the population aged 16–74)	88,30%	78%
Enterprises with their own website	78,30%	38,20%
R&D expenditure (% of GDP)	2,26%	0,32%

Sources: Eurostat (2024), UNDP (2024)

As shown in Table 2, the largest discrepancies between Ukraine and the EU are evident in business digitalisation (38.2% versus 78.3%) and innovation financing (0.32% versus 2.26% of GDP). These disparities directly impact the ability of Ukrainian enterprises to comply with the requirements of the GDPR and the AI Act. These indicators suggest that regulatory changes must be accompanied by the development of digital infrastructure and investment in human capital. The limited investment in R&D in Ukraine (0.32% of GDP) creates a structural barrier to meeting the stringent regulatory standards set out

in the EU AI Act. Finally, an analysis of global rankings highlights the challenges posed by the institutional environment. According to reports by the WIPO, Ukraine fell from 45th place to 60th place in the Global Innovation Index (GII) between 2020 and 2024. The key area of concern remains 'institutions', where the country ranks 107th (WIPO, 2024). Meanwhile, Ukraine's overall digital readiness score stands at 55.32 points according to the Network Readiness Index (NRI 2024), placing it 43rd among 133 countries. The highest score is recorded for the 'People' component (51.83 points), reflecting a relatively high level of digital literacy among the population. In contrast, the 'Governance' component (63.14 points) and particularly the 'Business' component (34.67 points) are considerably weaker (Portulans Institute, 2024). Therefore, despite the population's relatively high level of digital competence, Ukraine's overall level of digital integration remains below the EU average due to persistent institutional and economic constraints.

The identified disparities directly impact the economic returns from digital transformation. A low level of business digitalisation, coupled with inadequate investment in research and development, restricts businesses' ability to adopt new technologies, develop their own digital products, and expand innovative business models. In such circumstances, businesses may perceive regulatory requirements relating to data protection and the use of artificial intelligence primarily as an additional financial burden rather than as a factor that contributes to long-term competitiveness. At the same time, insufficient digitalisation generates higher transaction costs for Ukrainian businesses and widens the productivity gap relative to enterprises in EU Member States. In this context, investment in digital infrastructure, research and development, and human capital should be seen as key drivers of economic growth, rather than as ancillary components of regulatory adaptation. Combining these factors can reduce the costs of digital transformation for businesses, improve the efficiency of data use, and facilitate the integration of Ukrainian companies into European value chains.

This is particularly significant under martial law, when limited financial resources, infrastructure destruction and increased investor risk exacerbate the structural disparities of the digital economy. Therefore, Ukraine's economic policy on digital transformation should not only seek to reduce the technological gap with the EU, but also the investment and productivity gaps. From this perspective, the harmonisation of the digital environment with European standards only has substantive economic significance if it is accompanied by greater access for businesses to financing, digital infrastructure, technology and qualified human capital.

This article also discusses the economic implications and variations in the regulatory strategies adopted

by the EU and Ukraine. The EU's regulatory model is significant in both legal and economic terms. Predictable digital regulation reduces information asymmetry between the state, businesses and investors, lowers transaction costs and fosters stable conditions for the growth of digital markets. This regulatory environment is underpinned by the GDPR, the AI Act, the DSA and the DMA. The GDPR establishes uniform rules for the protection of personal data. The AI Act takes a risk-based approach to regulating artificial intelligence systems. Meanwhile, the DSA and DMA establish rules governing the operation of digital platforms and constrain the exercise of their market power. Furthermore, Ukraine is developing a comprehensive regulatory system for the digital economy. The Law of Ukraine 'On Personal Data Protection' requires updating to align with GDPR standards. Although the Concept for the Development of Artificial Intelligence in Ukraine has been approved, dedicated AI regulation is currently absent. Competition law only partially considers the specific characteristics of digital platform operations. Although the Law of Ukraine 'On Virtual Assets' has been adopted, it has not yet come into force due to the absence of the necessary tax framework. This has created regulatory uncertainty in the crypto-asset market. Meanwhile, work is ongoing on new legislation in the field of personal data protection, as well as on adapting national regulations to align with EU legislation.

The current regulatory framework creates additional regulatory risk. It reduces the investment appeal of the digital sector, increases business compliance costs and impedes Ukraine's integration into the European digital market. Consequently, legal uncertainty becomes an economic factor that hinders the development of digital entrepreneurship, innovative activity and investment inflows.

The following recommendations are proposed for harmonising Ukrainian legislation with European standards, based on the analysis conducted.

5. Conclusions

The findings of the study demonstrate that legal and ethical conflicts within the digital economy possess a direct economic dimension. The impact of these technologies is manifest in a number of ways, including the complexity of regulating technological processes, shifts in transaction costs, levels of regulatory risk, investment activity, business competitiveness, and the adoption rate of digital innovations. Consequently, the quality of the institutional environment should be regarded as a critical determinant of the economic efficiency of digital transformation.

The study systematically identifies three key types of conflicts in the digital economy: firstly, between privacy and data monetisation; secondly, between algorithmic autonomy and the economic allocation of risks; and thirdly, between digital security and economic efficiency. Each of these conflicts generates a distinct set of economic consequences.

The first of these concerns the relationship between the economic value of data and the costs associated with its proper use and protection. The second addresses the allocation of risks, financial losses, and costs arising from errors in algorithmic systems. The third highlights the need to balance cybersecurity costs, business continuity, and the risks of economic loss resulting from digital incidents.

The developed cyclical model, illustrating the formation and resolution of ethico-legal conflicts, demonstrates that technological innovation → ethical conflict → legal uncertainty → economic consequences → regulatory intervention constitutes a recurring mechanism in the development of the digital environment. The pivotal economic component of this cycle pertains to legal uncertainty, which has been demonstrated to engender elevated transaction costs, impede the evaluation of investment risks, and potentially prolong decisions regarding the adoption of novel technologies. Concurrently, effective regulation is

Table 3

Directions for Harmonising Ukrainian Legislation

Problem	EU Standard	Current Situation in Ukraine	Recommendation
Personal data protection	GDPR	Outdated legislation	Adopt a new law aligned with the GDPR
AI regulation	AI Act	Concept adopted; no dedicated legislation	Adopt an AI law based on a risk-based approach
Digital platform operations	DSA, DMA	Weak regulation	Strengthen competition law enforcement
Virtual assets	MiCA	Law adopted but not yet in force	Bring the law into force and introduce necessary tax amendments
Digital rights protection	Independent supervisory authorities	No specialised authority	Establish an independent digital rights protection authority
Innovation testing	Regulatory sandboxes	Non-existent	Introduce regulatory sandboxes

Source: compiled by the authors

capable of reducing uncertainty and establishing more predictable conditions for investment and innovation. Consequently, regulatory policy in the digital economy should be regarded not merely as a risk-mitigation mechanism, but also as an instrument for fostering a favourable economic environment.

A comparison between Ukraine and the European Union revealed significant differences in technology, investment and institutions. The differences in the level of business digitalisation and R&D funding are particularly indicative: while 38.2% of Ukrainian enterprises have a corporate website, this figure is 78.3% in the EU. Furthermore, Ukraine's R&D expenditure amounts to just 0.32% of GDP, compared to 2.26% in the EU. These disparities demonstrate that regulatory adaptation alone cannot ensure digital convergence. The economic impact depends on the availability of financial resources, digital infrastructure and human capital, as well as the capacity of enterprises to invest in technological upgrades.

The European experience shows that a coordinated regulatory environment can serve as the economic infrastructure of a digital market. The GDPR, AI Act, DSA and DMA introduce clearer rules for those operating in the digital economy, reducing regulatory uncertainty and creating a fairer environment for competition. For Ukraine, therefore, harmonisation with European approaches is significant not only as a means of fulfilling European integration commitments, but also as a way of reducing institutional barriers to investment, fostering digital entrepreneurship and integrating Ukrainian companies into European value chains. The mechanical transposition of European regulatory requirements alone cannot ensure the expected economic outcomes. In light of insufficient business digitalisation, limited R&D funding and heightened security risks, new requirements could exacerbate the short-term regulatory burden on businesses. Therefore, harmonisation must be accompanied by economic instruments that support digital transformation. These instruments should include investment incentives for digital infrastructure and human capital development, as well as support for innovative enterprises and expanded access to digital technologies for small and medium-sized enterprises (SMEs).

In the context of martial law, this approach assumes particular significance. Digital infrastructure and services have been identified as key drivers of economic resilience, with the potential to ensure the continuity of business processes, reduce coordination costs, and enable enterprises to adapt to external shocks. Concurrently, war-related risks have been shown to exacerbate regulatory and investment uncertainty. Therefore, it is vital that digital transformation policy addresses the requirements of economic security,

innovative development, and competitiveness simultaneously.

Accordingly, the study's main finding is that the effectiveness of digital regulation should be assessed not only by the extent to which Ukrainian legislation is formally harmonised with European Union law, but also by its economic outcomes. These outcomes include reduced transaction and regulatory costs, increased investment activity, greater business digitalisation, stimulated innovation, enhanced competitiveness and a more resilient digital economy. Therefore, shifting the focus from the number of legal provisions implemented to their economic impact could provide the basis for an effective model of Ukraine's digital integration into the European Union.

The study's findings support the following conclusions. The European Union has established a comprehensive regulatory framework for the digital economy, comprising the GDPR, the AI Act, the DSA and the DMA. This framework strikes a balance between innovation and the development of digital markets, while also protecting human rights. In contrast, Ukraine is still in the process of adapting its legislation to align with European standards, particularly with regard to the protection of personal data, the regulation of artificial intelligence, and the operation of digital platforms.

An analysis of statistical indicators of digital transformation (Eurostat, DESI, UNDP, WIPO and NRI) revealed significant discrepancies between Ukraine and EU averages in terms of business digitalisation, innovation activity and institutional capacity. For example, 38.2% of Ukrainian enterprises have their own website, compared with 78.3% in the EU; R&D expenditure amounts to 0.32% of Ukraine's GDP, compared with 2.26% in the EU; and Ukraine ranks 107th for the 'Institutions' pillar in the 2024 Global Innovation Index. This complicates the harmonisation of digital legislation and increases the regulatory risks associated with developing the digital economy.

The developed typology of ethico-legal conflicts and the proposed cyclical model of their development can be used as analytical tools to assess the economic consequences of digital regulation, prepare regulatory amendments, design a roadmap to harmonise Ukrainian legislation with EU law and formulate digital transformation strategies under martial law.

The findings confirm that the quality of digital regulation is critical to international competitiveness, influencing regulatory risk, investment activity, transaction costs and the development of digital markets.

Future research should focus on empirically assessing the economic consequences of adopting AI in Ukraine, analysing the effectiveness of regulatory sandboxes after they have been implemented, and examining the impact of martial law on the protection of digital human rights.

References:

- Borovyk, A., Borovyk, L., & Derevianko, N. (2026). Monopolization of the information market by digital platforms: Legal and economic implications for media pluralism. *Baltic Journal of Economic Studies*, 12(2), 41-49. <https://doi.org/10.30525/2256-0742/2026-12-2-41-49>
- Dealroom. (2024). *Baltic Startup Funding Report 2024*. <https://dealroom.co>
- European Commission. (2023–2024). *Digital Economy and Society Index (DESI) reports*. Brussels: European Commission. <https://digital-strategy.ec.europa.eu/en/policies/desi>
- European Parliament & Council of the European Union. (2016). *General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)*. *Official Journal of the European Union*, L 119, 1-88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Parliament & Council of the European Union. (2022). *Digital Markets Act (DMA) (Regulation (EU) 2022/1925)*. *Official Journal of the European Union*, L 265, 1-66. <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- European Parliament & Council of the European Union. (2022). *Digital Services Act (DSA) (Regulation (EU) 2022/2065)*. *Official Journal of the European Union*, L 277, 1-102. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- European Parliament & Council of the European Union. (2024). *Artificial Intelligence Act (AI Act) (Regulation (EU) 2024/1689)*. *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Eurostat. (2024). *Digital economy and society statistics – EU member states*. Luxembourg: Publications Office of the European Union. <https://ec.europa.eu/eurostat/web/digital-economy-and-society>
- Eurostat. (2024). *Digital economy and society statistics – Eastern Partnership countries*. Luxembourg: Publications Office of the European Union. <https://ec.europa.eu/eurostat/web/digital-economy-and-society>
- Kapuliak, V., Shapovalova, I., & Kavunska, A. (2026). Digital human rights in the digital economy: Legal and economic aspects. *Baltic Journal of Economic Studies*, 12(2), 405-412. <https://doi.org/10.30525/2256-0742/2026-12-2-405-412>
- Menshikov, V., Ruza, O., & Semeneca, J. (2026). Artificial intelligence and inequality in the startup economy: A conceptual framework for digital stratification. *Baltic Journal of Economic Studies*, 12(2), 458-468. <https://doi.org/10.30525/2256-0742/2026-12-2-458-468>
- Ministry of Digital Transformation of Ukraine. (n.d.). *Portal 'Diia': Electronic public services*. <https://diia.gov.ua>
- OECD. (2024). *OECD Digital Economy Outlook 2024*. Paris: OECD Publishing. <https://doi.org/10.1787/a1689dc5-en>
- Portulans Institute. (2024). *Network Readiness Index 2024: Ukraine profile*. <https://networkreadinessindex.org/countries/ukraine/>
- Posner, R. A. (2014). *Economic analysis of law* (9th ed.). New York: Wolters Kluwer.
- Srnicek, N. (2016). *Platform capitalism*. Cambridge: Polity Press.
- Tytska, Y., Anisimov, V., & Matvieiev, O. (2026). Economic systems in the context of digitalisation and AI: Theoretical and legal modelling. *Baltic Journal of Economic Studies*, 12(2), 210-217. <https://doi.org/10.30525/2256-0742/2026-12-2-210-217>
- UNDP. (2024). *Report on the use of electronic services in Ukraine*. Kyiv: United Nations Development Programme. <https://www.undp.org/ukraine>
- The Law of Ukraine 'On Personal Data Protection' of June 14, 2025, No. 2297-VI. Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2010, No. 34, Art. 481. <https://zakon.rada.gov.ua/laws/show/2297-17>
- The Law of Ukraine 'On Electronic Communications' of 30.05.2026, No. 1089-IX. <https://zakon.rada.gov.ua/laws/show/1089-20>
- The Law of Ukraine 'On Virtual Assets' of 15.11.2024, No. 2074-IX. Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2023, No. 15, Art. 51. <https://zakon.rada.gov.ua/laws/show/2074-20>
- The Law of Ukraine 'On Media' of 16.09.2026, No. 2849-IX. Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2023, No. 47-50, Art. 120. <https://zakon.rada.gov.ua/laws/show/2849-20>
- World Bank. (2024). *World Development Report 2024: Digital Development*. Washington, DC: World Bank Group.
- World Intellectual Property Organization (WIPO). (2024). *Global Innovation Index 2024: Ukraine profile*. Geneva: WIPO. https://www.wipo.int/global_innovation_index/en/
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.