МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

Науковий журнал

Том 16, № 2
2026

Київ
2026

ISSN 2519-4216
E-ISSN 2519-4313

УДК 34
DOI: 10.63341/naia-chasopis/2.2026

Засновник:
Національна академія внутрішніх справ
Рік заснування: 2011

Виходить чотири рази на рік

Рекомендовано до друку та поширення через мережу Інтернет Вченою радою Національної академії внутрішніх справ (протокол № 10 від 26 травня 2026 р.)

Ідентифікатор медіа в Реєстрі суб'єктів у сфері медіа R30-02448
Рішення Національної ради України з питань телебачення і радіомовлення від 11 січня 2024 року № 26

Журнал входить до переліку наукових фахових видань України
Категорія «Б». Кластер "Право". Спеціальності: D8 – Право, D9 – Міжнародне право (наказ МОН України № 928 від 11.06.2026)

Журнал представлено в міжнародних наукометричних базах даних, репозитаріях та пошукових системах: COPE, ERIH PLUS, SOLO, UCSB Library, Google Scholar, CrossRef, Worldcat, Dimensions, Litmaps, Cambridge University Library, University of Oslo Library, University of Hull Library, European University Institute, Leipzig University Library, OUCI, НБУ ім. В.І. Вернадського, Фахові видання України, Електронний репозитарій НАВС

Юридичний часопис Національної академії внутрішніх справ : наук. журн. / [редкол.: С. Чернявський (голов. ред.) та ін.]. – Київ : Нац. акад. внутр. справ, 2026. – Т. 16, № 2. – 91 с.

Адреса редакції:
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
Тел.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/uk

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
NATIONAL ACADEMY OF INTERNAL AFFAIRS

LAW JOURNAL

OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS

Scientific Journal

Volume 16, No. 2
2026

Kyiv
2026

ISSN 2519-4216
E-ISSN 2519-4313

UDC 34
DOI: 10.63341/naia-chasopis/2.2026

Founder:
National Academy of Internal Affairs
Year of foundation: 2011

Published four times per year

Recommended for printing and distribution
via the Internet by the Academic Council
of National Academy of Internal Affairs
(Minutes No. 10 of May 26, 2026)

Media identifier in the Register of Media Entities R30-02448
Decision of the National Council of Ukraine on Television and Radio Broadcasting
of 11 January 2024 No. 26

The journal is included in the list of scientific professional publications of Ukraine
Category "B". Cluster: Law. Speciality: 0421 – Law.
(Order of the Ministry of Education and Science of Ukraine No. 928 of 11 June 2026)

The journal is presented international scientometric databases, repositories and scientific systems: COPE, ERIH PLUS, SOLO, UCSB Library, Google Scholar, CrossRef, Worldcat, Dimensions, Litmaps, Cambridge University Library, University of Oslo Library, University of Hull Library, European University Institute, Leipzig University Library, OUCI, Vernadsky National Library of Ukraine, Professional publications of Ukraine, Electronic repository NAIA

Law Journal of the National Academy of Internal Affairs / Ed. by S. Cherniavskyi (Editor-in-Chief) et al. Kyiv: National Academy of Internal Affairs, 2026. Vol. 16, No. 2. 91 p.

Editors office address:
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
Tel.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/en

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ
Том 16, № 2

Редакційна колегія

LAW JOURNAL
OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS
Volume 16, No. 2

Editorial Board

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ
Том 16, № 2

ЗМІСТ

LAW JOURNAL
OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS
Volume 16, No. 2

CONTENTS

UDC 343.9:343.35:351.74
DOI: 10.63341/naia-chasopis/2.2026.09

ISSN 2519-4216
E-ISSN 2519-4313

Prospects for the implementation of European experience in combating organised crime in Ukraine: Theoretical, managerial and legal foundations of state regulation in the field of national security

Oleksii Kopan*
Doctor of Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-0797-7952

Vladyslav Melnyk
PhD in Law, Associate Professor
Institute of Scientific Research on Civil Protection
of the National University of Civil Protection of Ukraine
02000, 21 Vyshhorodska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-2659-9942

Abstract
This article analyses contemporary approaches to combating organised crime, with a focus on ensuring the resilience of the security system. It identifies key elements of resilience, adaptive mechanisms and strategic priorities in the context of transformational threats. The integration of the concept of resilience into state criminal policy and international cooperation is examined. The aim of the article was to study the theoretical, legal and managerial foundations for implementing European experience in combating organised crime in Ukraine through the prism of ensuring the resilience of national security. The research methodology was based on the use of formal-logical, systemic and comparative legal analysis, as well as methods of content analysis of international strategic documents and statistical data. The study summarises the approaches of leading European countries to combating organised crime and identifies key directions for adapting this experience in the context of contemporary challenges and threats. Particular attention was paid to the role of EU institutions in shaping security policy and the possibilities for their integration into Ukraine's legal system. This made it possible to identify the distinctive features of European models for preventing and combating criminal organisations, their interaction with state and civil society institutions, as well as mechanisms for ensuring the resilience of the security system. It has been confirmed that effective counteraction to organised crime requires a combination of legal, managerial, technological and social tools. It has been demonstrated that the integration of EU experience into Ukrainian legislation is possible provided that the regulatory framework is

Article's History:
Received: 09.01.2026
Revised: 14.04.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Kopan, O., & Melnyk, V. (2026). Prospects for the implementation of European experience in combating organised crime in Ukraine: Theoretical, managerial and legal foundations of state regulation in the field of national security. *Law Journal of the National Academy of Internal Affairs*, 16(2), 9-17. doi: 10.63341/naia-chasopis/2.2026.09.

*Corresponding author (*kopan_a@ukr.net*)

harmonised, modern digital technologies are introduced into the field of criminal analytics, and the level of inter-agency coordination is enhanced. The concept of a "resilient security system" has been formulated as an adaptive institution capable of effectively responding to transnational threats and hybrid challenges. The practical significance lies in the development of proposals for integrating territorial defence into Ukraine's national security architecture and the implementation of European standards into national legislation

Keywords:
resilience of the security system; organised crime; national security; European experience; territorial defence; legal regulation

Introduction

Countering organised crime is regarded not merely as a distinct area of criminal policy but as a component of the state's capacity to guarantee security, economic resilience, and institutional trust. For Ukraine, this issue has been exacerbated by the full-scale war, population displacement, the illicit arms trafficking, the shadowing of logistics flows and the growing role of digital platforms in criminal activity. An additional risk is posed by the transformation of organised groups into flexible network structures that combine illicit markets with legitimate business, corrupt ties and cross-border coordination. Under such conditions, the effectiveness of the state's response depends not only on the criminalisation of acts, but also on the quality of interagency cooperation, analytical infrastructure, financial monitoring and international legal assistance. For a state simultaneously undergoing security transformation and adaptation to the European Union's acquis, the issue of adopting European models for combating organised crime has taken on both practical and theoretical-managerial significance.

In contemporary literature, organised crime has increasingly been interpreted as an adaptive network system rather than as a collection of isolated, stable groups. M. Bouchard (2020) examined the networked nature of organised crime and concluded that effective state intervention requires institutional flexibility and targeted influence on coordination nodes, rather than merely increasing repressive pressure. The author demonstrated that criminal networks simultaneously combine cooperation and competition, so counter-crime policy must take into account the internal volatility of criminal ties. J. Ayling (2021), drawing on Australian practice, substantiated the advantages of shifting from a purely punitive model to a preventive one, focused on reducing opportunities for criminal markets to operate.

Researchers examining the economic and institutional dimensions of the problem emphasised the close link between organised crime, legal markets and the quality of governance. P. Campana & G.A. Antonopoulos (2024) proposed a relational approach, within which organised crime is viewed through the lens of configurations of ties, intermediation and access to resources, rather than solely through the formal characteristics of a criminal organisation. The issues of digitalisation and the cross-border nature of criminal practices were actively explored in the research of R. Adel (2024), who substantiated the concept of "digital organised crime" and demonstrated that the digital environment alters not only the ways in which crimes are committed, but also the methods used to investigate and prevent them. O. Farion *et al*. (2023), analysing cross-border crime in border regions, demonstrated that the effectiveness of strategies is enhanced when criminal analysis, inter-agency data sharing and international cooper ation are combined. A separate section of studies was devoted to crisis, war and social prevention aspects. Researchers M. Pardal *et al*. (2023) demonstrated that during periods of crisis, illicit markets do not disappear but rather reorient themselves, utilising new logistical routes and distribution channels. According to R. Muggah (2023), armed conflicts accelerate the interpenetration of organised crime, violence and shadow governance. H.T. Luong (2024) demonstrated that, in the context of weak control over the prison and local security systems, criminal structures are capable of evolving from prison gangs into transnational networks.

Ukrainian researchers have focused primarily on the security transformation of the state and the European adaptation of institutions. A. Murashko (2021) analysed global trends in state policy in the field of security and defence and concluded that the role of integrated threat management is growing. Meanwhile, H.T. Luong (2020), examining the dynamics of transnational crime in South-East Asia, as well as A. Ofusori & P. Hendradi (2023), analysing the spatial and communicative mechanisms of concealing criminal activity, demonstrated that effective policy must go beyond formal criminal law responses. Also important for public perception of the issue is the study by Travaglino *et al.* (2025), which showed that citizens' perceptions of organised crime significantly influence the legitimacy of anti-crime policy.

Thus, the current state of scientific knowledge has demonstrated significant progress in the study of the networked, digital, preventive and security aspects of organised crime; however, the issue of the comprehensive adaptation of European models to the Ukrainian national security system in the context of war and European integration remains insufficiently explored. The limits of the permissible involvement of security and defence institutions in countering criminal threats

beyond the scope of traditional law enforcement jurisdiction also remain insufficiently defined.

The aim of the study was to define the theoretical, managerial and legal foundations for implementing European experience in combating organised crime in Ukraine, taking into account the needs of national resilience. To achieve this aim, three objectives were formulated: to identify which features of modern organised crime are of decisive importance for state regulation; to ascertain which elements of European experience can be adapted to the Ukrainian institutional model; and to outline the regulatory and administrative changes necessary for their practical implementation.

Materials and Methods

The object of the study was state regulation and institutional mechanisms for combating organised crime in Ukraine, whilst the subject was the theoretical, legal and managerial foundations for implementing European experience within the national security system. The conceptual framework of the study comprised three interrelated approaches. The first was a network approach, which allowed organised crime to be analysed as a configuration of connections, roles and resources, rather than merely as a collection of formally defined criminal organisations. The second was a resilience approach, within which the ability of state institutions to adapt to complex criminal threats without losing key functions was assessed. The third is the institutional-managerial approach, which focused the research on analysing coordination, information exchange, the responsibilities of actors, and strategic planning tools.

Methodologically, formal-legal, comparative-legal, systemic-structural and content-analytical methods were combined. The formal-legal method was applied to analyse the content of the Law of Ukraine "On Organisational Legal Principles of Struggle against the Organised Crime"[1], Criminal Code of Ukraine[2], as well as related legislation in the fields of cybersecurity, financial monitoring and international legal assistance. The comparative legal method was used to compare Ukrainian approaches with the EU Strategy to Tackle Organised Crime 2021-2025[3]. To verify the conclusions regarding digitalisation and international cooperation, publicly available analytical materials from the European Union Agency for Law Enforcement Cooperation (2025) and the Internet Organised Crime Threat Assessment (IOCTA) (2026) were also utilised.

The research process comprised four stages. In the first stage, contemporary academic approaches to understanding organised crime were summarised, and concepts suitable for analysis were identified: networked criminality, governance approach, resilience and dynamic decision-making. In the second stage, the Ukrainian regulatory framework was analysed, and institutional nodes were identified where there are overlaps in powers or gaps in coordination. In the third stage, the Ukrainian model was compared with European practices – criminal analytics, joint investigation teams, financial investigations, preventive tools and digital information exchange. In the fourth stage, recommendations were formulated, the content of which correlated with the results of the previous analysis and did not go beyond the scope of the materials actually examined.

Results

The analysis carried out has shown that, for Ukraine, the decisive factor is not so much the formal increase in specific types of crime as the change in the way criminal activity is organised. In Europol's public reports, notably those of the European Union Agency for Law Enforcement Cooperation (2025) and the Internet Organised Crime Threat Assessment (IOCTA) (2026), it is emphasised that modern criminal networks combine violent, economic and digital forms of activity, actively utilising legal business structures, anonymised communication services, crypto-assets and instruments of corruption. These conclusions are consistent with the theoretical propositions of M. Bouchard (2020) and P. Campana & G.A. Antonopoulos (2024), which allow organised crime to be viewed as a system of flexible connections capable of rapidly reconfiguring itself following external intervention. In the Ukrainian context, this meant that a response model focused primarily on detecting completed criminal offences proved insufficient without tools for the early detection of network activity, financial analytics and inter-agency data sharing.

Materials from Ukrainian security and law enforcement agencies for the years 2022-2024 showed that martial law had heightened the risks of illicit arms trafficking, smuggling channels, shadow logistics, fraudulent schemes in the digital environment, and the exploitation of humanitarian or defence supply chains for criminal enrichment. An analysis of official reports from Ukraine's law enforcement and security agencies confirms that martial law has significantly increased the risks of illicit arms trafficking, smuggling channels, shadow logistics, and fraudulent schemes in the digital environment. Data from the National Police of Ukraine (2023) show a significant increase in cases of illicit trafficking in weapons and ammunition, linked to the expansion of arsenals and illegal supply networks.

[1] Law of Ukraine No. 3341-XII "On Organisational Legal Principles of Struggle against the Organised Crime". (1993, June). Retrieved from https://zakon.rada.gov.ua/laws/show/3341-12?lang=en#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "On the EU Strategy to tackle Organised Crime 2021-2025". (2021, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0170.

Concurrently, the Centre for Security Studies (CENSS) (2024) noted in its 2024 monitoring reports that organised criminal groups are adapting their schemes to current conditions and actively using digital channels and postal services to move weapons and ammunition.

In the area of smuggling and illicit schemes involving humanitarian and defence cargo, the Economic Security Bureau of Ukraine (2023) uncovered cases of illegal imports of goods disguised as humanitarian aid, which were subsequently misused or ended up on the black market. Similarly, investigations by the National Anti-Corruption Bureau of Ukraine (2024) uncovered organised schemes to evade customs procedures at the border, indicating abuse of the customs system for the smuggling of goods. The excessive burden on law enforcement agencies in wartime also creates a fertile ground for the development of fraudulent schemes in the digital environment, in particular fake platforms and transactions that exploit citizens' crisis-driven sentiments and information uncertainty. All these factors point to a transformation of organised crime in Ukraine, where traditional risks are exacerbated by new forms of shadow economic activity during martial law. In this regard, R. Muggah's (2023) conclusions regarding the convergence of organised crime and situations of armed violence have been particularly clearly confirmed by the example of Ukraine. M. Pardal *et al*. (2023) convincingly demonstrated that crises do not destroy illegal markets, but rather alter routes, intermediaries and forms of concealment, and it is precisely this logic that has been observed in wartime conditions. Consequently, the focus of state intervention should have been not only on individual groups but also on infrastructure – financial, communications, transport and corruption-related.

A comparative legal analysis has shown that the European approach to combating organised crime has not been limited to tightening criminal liability. The EU Strategy to tackle Organised Crime 2021-2025[1] guided Member States towards dismantling criminal business models, strengthening digital investigative tools, asset confiscation, coordinating financial investigations and building international cooperation. This approach aligns with the findings of J. Ayling (2021), according to which preventive and environmental measures often prove more effective than a purely punitive response. Similarly, M. Pardal *et al*. (2023) concluded that preventive tools are effective when they simultaneously reduce access to resources, recruitment channels, and institutional "windows of opportunity" for criminal groups.

A key feature of European approaches has been the reliance on criminal analytics and robust information sharing. A. Di Nicola *et al.* (2025) convincingly demonstrated that, in a digital society, organised crime is shifting to environments where traditional investigative tools lose their effectiveness, and therefore new analytical methods, access to large datasets, and technologies for detecting risk patterns are required. The conclusion by J. Kerstholt *et al.* (2024) regarding the need for dynamic decision-making also had direct practical value: in situations where criminal networks rapidly change communication channels, financial instruments and intermediaries, decisions by law enforcement agencies must be made not as one-off actions, but as a continuous cycle involving constant adjustment. This explained why European institutions, including Europol and Eurojust, place such emphasis on information-sharing platforms, joint analytical products and cross-border investigation teams.

Of particular interest to Ukraine was the example of countries that have combined the fight against organised crime with policies on economic security and local resilience. R. Leukfeldt *et al.* (2017), analysing the interconnection between organised, financial and property crime, demonstrated that effective state policy must focus on assets, beneficial ownership structures, real estate and money laundering schemes, as it is precisely there that criminal networks conceal their presence in the legal economy. For Ukraine, this meant the need to move from a narrow criminal procedural approach to an integrated model combining law enforcement, financial, regulatory and local levels of governance.

An examination of the Ukrainian regulatory framework revealed that current regulation remains fragmented. Law of Ukraine No. 3341-XII[2] etains its status as a foundational act, but its structure is shaped by the institutional architecture of the 1990s and does not fully reflect contemporary digital, financial and cross-border risks. The Criminal Code of Ukraine[3] establishes liability for the creation of a criminal organisation, money laundering, terrorist activities and related offences; however, this is insufficient for the systematic regulation of issues concerning intelligence sharing, risk management, the use of digital evidence and the coordination of the work of various authorities. It is precisely this problem that was highlighted by R. Adel (2024), O. Farion *et al*. (2023) and H.T. Luong (2020): in a transnational and digital environment, the state requires not only punitive provisions but also legal mechanisms that facilitate operational coordination and information gathering.

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "On the EU Strategy to tackle Organised Crime 2021-2025". (2021, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0170.

[2] Law of Ukraine No. 3341-XII "On Organisational Legal Principles of Struggle against the Organised Crime". (1993, June). Retrieved from https://zakon.rada.gov.ua/laws/show/3341-12?lang=en#Text.

[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.

It has also been established that there are three key issues within the Ukrainian model. The first is institutional duplication, whereby several bodies simultaneously hold overlapping powers in the areas of anti-corruption, economic crime, terrorism and organised crime, yet lack a fully-fledged shared analytical platform. The second is the insufficient integration of financial investigations into the logic of combating organised groups, although European approaches are based precisely on the "follow the money" concept. The third is the limited access to international information exchange in a manner commensurate with the needs of wartime and cross-border investigations. In this regard, the findings of R. Roks *et al.* (2021) and A. Ofusori & P. Hendradi (2023) was instructive: criminal groups actively exploit spatial gaps, local contacts and informal codes of silence; thus, without combining operational work, analysis and local prevention, the state's response remains belated.

Based on the analysis conducted, it was established that the adaptation of European experience in Ukraine should not take place through the mechanical copying of individual institutions, but through the coordinated modernisation of the law, governance and analytical infrastructure. Firstly, it is advisable to adopt a separate strategic document – the National Strategy for Combating Organised Crime until 2030 – which would define a unified conceptual framework, state policy priorities, coordination mechanisms and performance indicators. Secondly, a mechanism for inter-agency criminal intelligence requires regulatory consolidation, with a clear demarcation of data access, exchange standards and responsibility for their use. Thirdly, provisions of Ukrainian legislation in the areas of financial monitoring, asset confiscation, digital evidence and joint investigations with EU states require harmonisation.

These conclusions were consistent with the works of J. Cubides-Cardenas *et al*. (2025), in which regional cooperation was viewed as a prerequisite for the sustainable deterrence of transnational crime, as well as with the study by G.A. Travaglino *et al*. (2025), which emphasised the importance of public legitimacy for anti-crime policy. In practice, this meant that, alongside purely law enforcement measures, it was necessary to enhance the transparency of procedures, local prevention programmes, and cooperation with the banking sector, customs authorities, local government bodies and international partners. The role of territorial defence forces and other security structures within this system was to be viewed as limited and supportive – primarily in terms of protecting critical infrastructure, strengthening security measures in border and frontline areas, identifying risky logistical anomalies, and supporting community resilience. Granting such entities independent law enforcement functions in the fight against organised crime would not be consistent with the principle of a clear division of jurisdictions.

Discussion

The findings confirmed that the most productive analytical framework for understanding organised crime in the Ukrainian context is a combination of network, institutional and security approaches. In this respect, the study's conclusions align with the positions of M. Bouchard (2020), N. Breuer & F. Varese (2023) and P. Campana & G.A. Antonopoulos (2024), who proposed basing analysis not on a formal classification of groups, but on the nature of their connections, access to resources and methods of embedding themselves in legal markets. For Ukraine, this perspective was particularly important, as martial law created numerous "friction zones" between security, logistics, the economy and the digital environment, within which criminal actors are capable of operating in a hybrid manner. It is precisely for this reason that the conclusion regarding the need to transition to integrated governance, rather than maintaining an exclusively criminal law model, should be regarded not as a theoretical generalisation, but as a practical requirement.

At the same time, the study has helped to clarify exactly how resilience should be understood in the context of combating organised crime. In contrast to a simplistic approach, where resilience is interpreted as a system's ability to withstand shocks without altering its own structure, the study's findings align with the conclusions of J. Ayling (2009): resilience means the state's ability to rapidly adapt procedures, coordination channels and analytical tools in line with the dynamics of threats. In this sense, P. Finkenbusch (2024) rightly cautioned against the "naturalisation of danger", where references to resilience mask a lack of deep reforms. For Ukrainian practice, this meant that the slogan of enhancing national resilience is not sufficient in itself if it is not accompanied by concrete changes in data architecture, financial investigations, the separation of powers, and the legal framework for international cooperation.

The findings also provided grounds for a critical assessment of the idea of directly transplanting individual foreign models without adapting them to the Ukrainian institutional reality. J. Ayling (2021) and M. Pardal *et al.* (2023) have shown that preventive tools are effective only when they are embedded in a stable interagency environment and supported by relevant data. In EU countries, the prevention of organised crime relies on mature registers, established information-sharing practices, the role of local authorities, advanced financial investigations and constant liaison with European agencies. In Ukraine, however, some of these elements are either in the early stages of development or operate in a fragmented manner. Consequently, the practical conclusion is that the primary priority should be capacity-building rather than the declarative adoption of individual instruments.

This is confirmed by the digital dimension of the problem. The work of A. Di Nicola *et al.* (2025) has

convincingly demonstrated that the digital environment has transformed both organised crime itself and the methodology used to study it. Within the scope of the analysis conducted, this conclusion was further refined: for Ukraine, the digitalisation of the fight against organised crime cannot be limited to the development of the cyber police or the investigation of individual cybercrimes. What is required is the creation of an analytical infrastructure capable of integrating data on financial transactions, customs risks, telecommunications patterns, logistics chains and transnational contacts. The conclusion by J. Kerstholt *et al*. (2024) proved particularly relevant here: in the fight against adaptive networks, it is not a one-off reaction that matters, but a managed decision cycle that can change in line with the adversary's behaviour. Thus, digitalisation was interpreted not as a technical add-on to law enforcement activities, but as a new logic of risk management.

The discussion regarding the relationship between the national and international levels required separate attention. O. Farion *et al.* (2023) and J. Cubides-Cardenas *et al.* (2025) emphasised that cross-border crime cannot be effectively deterred by the forces of a single state, especially if illicit markets utilise regional transport corridors, financial hubs and differences in regulatory regimes. The present study confirmed this conclusion, but at the same time highlighted the limits of its applicability: international cooperation works only when the national system is capable of rapidly producing high-quality analytical outputs, properly documenting evidence and maintaining consistent channels of communication with partners. Without domestic institutional capacity, even expanding formal participation in Europol, Eurojust or joint investigation teams does not yield the expected results. Thus, recommendations regarding international integration were justified only in light of the need for domestic administrative and regulatory modernisation.

The issue of the local dimension of security has also proved contentious. R. Roks *et al.* (2021) demonstrated that criminal markets are embedded in specific locations – ports, transport hubs, warehouses, and border communities – while A. Ofusori & P. Hendradi (2023) showed how silence, social ties and local loyalty complicate the detection of criminal activity. For Ukraine, this had two consequences. Firstly, local administrations, self-governing bodies, and border and customs units must be regarded as participants in anti-crime policy, rather than merely as recipients of instructions from law enforcement agencies. Secondly, the involvement of territorial defence forces and other security institutions in maintaining community resilience can only be useful as a supplementary, clearly regulated mechanism that does not replace criminal investigations or operational-search activities. It is precisely this conclusion that distinguishes the present study from more declarative approaches, where any expansion of the security sector is automatically regarded as positive.

A comparison with international cases has also helped to clarify the significance of the social-preventive component. H.T. Luong (2024) demonstrated that organised crime can expand due to the weakness of control institutions in places of confinement, whilst H.T. Luong (2020) and R. Muggah (2023) showed that prolonged crises open up new channels for recruitment, logistics and the violent control of territories. It follows that, for Ukraine, anti-crime policy must not be limited to operational measures. It must include strengthening integrity within the prison system, customs control, the arms trade, defence procurement, as well as in areas where funds are laundered through property and business. This is precisely why the study's findings align with the arguments of R. Leukfeldt *et al.* (2017): without focusing on the financial and property presence of criminal networks, the dismantling of their organisational foundations remains incomplete.

Another aspect of the discussion concerned the public legitimacy of anti-crime policy. G.A. Travaglino *et al.* (2025) drew attention to the fact that citizens have different understandings of "organised crime", and this influences support for state measures. In the Ukrainian context, where the discourse on security often focuses on external threats, there is a risk of underestimating those criminal practices that operate through corruption, financial fraud or infiltration of legitimate business. Consequently, state policy must be not only effective but also communicatively clear: society needs to be shown why the fight against organised crime is an element of national security, economic stability and a just post-war recovery.

The analysis also highlighted the issue of criminal networks' economic infiltration into legal markets. R. Leukfeldt *et al*. (2017) specified this phenomenon using examples of property and financial schemes. Furthermore, the work by N. Breuer & F. Varese (2023) provided grounds for distinguishing between groups focused on the trade in illicit goods and groups that effectively perform informal governance functions in certain environments. For Ukraine, this distinction is methodologically important, as the response to drug trafficking, illegal arms, smuggling or money laundering cannot be identical. Accordingly, the state strategy must comprise separate components – law enforcement, financial, digital and local prevention – each with its own performance indicators.

Conclusions

The study found that European experience in combating organised crime is valuable to Ukraine not so much as a set of isolated repressive measures, but rather as a comprehensive model of integrated governance that encompasses prevention, analysis, financial investigations, international cooperation and inter-agency

coordination. The study confirmed that modern organised criminal structures operate as adaptive networked systems, capable of rapidly changing their methods of communication, channels for the illicit trafficking of goods, digital platforms and financial schemes under the influence of new technologies and crisis situations. In this context, traditional repressive methods used by law enforcement agencies prove insufficient, as they often fail to ensure the timely identification of risks, do not monitor digital and financial flows, and do not integrate information across different agencies and levels of management.

An analysis of European practices has shown that the effectiveness of combating organised crime is largely ensured through the application of comprehensive strategies that combine legal regulation with coordination between the police, financial institutions, judicial authorities and specialised analytical units. For Ukraine, this means the need to modernise not only criminal legislation but also procedures for inter-agency data exchange, the collection and processing of analytical information, as well as the introduction of uniform standards for financial monitoring and the processing of digital evidence. In particular, it has been established that effectively combining preventive measures with active investigations helps to reduce the scope for criminal organisations to infiltrate the legal economy and lowers the risks of financial crime, money laundering and smuggling.

The study also confirmed the need to adopt a national strategy to combat organised crime, which would integrate the approaches of various agencies, establish clear procedures for joint investigations and promote the harmonisation of national legislation with international standards. An important element of such a strategy should be the strengthening of local prevention, the protection of critical infrastructure and digital security, and raising public awareness of the risks of involvement in criminal schemes. At the same time, it is necessary to maintain a clear distinction between the functions of law enforcement agencies and security forces, so as not to create overlapping or conflicting competences.

The application of integrated approaches makes it possible to enhance Ukraine's national resilience in the face of contemporary threats, reduce opportunities for criminal groups to exert unlawful influence on the economy, improve the effectiveness of legal and analytical mechanisms, and create the conditions for Ukraine's more successful integration into the European security space. At the same time, the results obtained indicate that the adaptation of European practices requires a systematic approach, the incorporation of modern analytical technologies, the development of staff skills, and the assurance of transparency and coordination among all stakeholders. Thus, the comprehensive implementation of these recommendations can ensure an effective fight against organised crime and enhance the overall security of the state at national and international levels. Prospects for further research lie in a comprehensive study of the adaptive network structures of organised crime in Ukraine, with a focus on digital platforms, financial schemes and the inter-agency integration of preventive and analytical mechanisms.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Adel, R. (2024). Militarization and evolution of cybercrime in the Dark Net: Threats and countermeasures. *Cybersecurity*, 8(8), 91. doi: 10.3390/cybersecurity8080091.

[2] Ayling, J. (2009). Criminal organizations and resilience. *International Journal of Law, Crime and Justice*, 37(4), 182-196. doi: 10.1016/j.ijlcj.2009.10.003.

[3] Ayling, J. (2021). Combating organized crime aussie-style: From law enforcement to prevention. In H. Nelen & D. Siegel (Eds.), *Contemporary organized crime* (Vol. 18) (pp. 185-207). Cham: Springer. doi: 10.1007/978-3-030-56592-3_12.

[4] Bouchard, M. (2020). Collaboration and boundaries in organized crime: A network perspective. *Crime and Justice*, 49(1), 425-469.

[5] Breuer, N., & Varese, F. (2023). The structure of trade-type and governance-type organized crime groups: A network study. *The British Journal of Criminology*, 63(4), 867-888. doi: 10.1093/bjc/azac065.

[6] Campana, P., & Antonopoulos, G.A. (2024). A relational approach to organised crime. *Trends in Organized Crime*, 27, 229-234. doi: 10.1007/s12117-024-09534-4.

[7] CENSS. (2024). *Organized crime groups and weapons: Scope and risks in 2024*. Retrieved from https://censs.org/organized-crime-groups-and-weapons-scope-and-risks-in-2024/.

[8] Cubides-Cardenas, J., Hernández-Alvarado, C.E., Jimenez-Reina, J., & Roncancio-Bedoya, A.F. (2025). Regional cooperation against transnational organized crime: Challenges and opportunities in the Western Hemisphere. *Frontiers in Political Science*, 7, article number 1657969. doi: 10.3389/fpos.2025.1657969.

[9] Di Nicola, A., Baratto, G., & Vettori, B. (2025). Criminological definitions of organized crime on the digital test bench: Towards a physical-digital framework. *Trends in Organized Crime*. doi: 10.1007/s12117-025-09575-3.
[10] Economic Security Bureau of Ukraine. (2023). *ESBU in Kyiv region exposed the illegal importation of a truck under the guise of humanitarian aid for the Armed Forces*. Retrieved from https://esbu.gov.ua/en/news/esbu-in-kyiv-region-exposed-the-illegal-importation-of-a-truck-under-the-guise-of-humanitarian-aid-for-the-armed-forces.
[11] European Union Agency for Law Enforcement Cooperation. (2025). *The changing DNA of serious and organised crime*. Luxembourg: Publications Office of the European Union.
[12] Farion, O., Kupriyenko, D., & Demianiuk, Yu., & Nikitiuk, A. (2023). Combating cross-border organized crime in the border region of the state: Strategy development methodology. *Journal of Liberty and International Affairs*, 9(2), 246-263. doi: 10.47305/JLIA2392246f.
[13] Finkenbusch, P. (2024). Naturalizing insecurity: Resilience and drug-related organized crime in the Americas. *Trends in Organized Crime*, 27(2), 197-211. doi: 10.1007/s12117-022-09454-1.
[14] Internet Organised Crime Threat Assessment (IOCTA). (2026). *The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime.* Luxembourg: Publications Office of the European Union.
[15] Kerstholt, J., Keijser, B., Veldhuis, G., & SmitsClijsen, E. (2024). Organized crime requires dynamic decision making. *Frontiers in Psychology*, 15, article number 1205135. Retrieved from doi: 10.3389/fpsyg.2024.1205135.
[16] Leukfeldt, R., Lavorgna, A., & Kleemans, E.R. (2017). Financial cybercrime as organized crime: Evidence from case studies and empirical data. *European Journal on Criminal Policy and Research*, 23(2), 165-183. doi: 10.1007/s10610-016-9332-z.
[17] Luong, H.T. (2020). Transnational Crime and its Trends in South-East Asia: A Detailed Narrative in Vietnam. *International Journal for Crime, Justice and Social Democracy*, 9(2), 88-101. doi: 10.5204/ijcjsd.v9i2.1504.
[18] Luong, H.T. (2024). Trends and patterns in online organized crime: A bibliometric review of Darknet-related studies. *International Journal of Cyber Criminology*, 18(1), 45-67. doi: 10.1057/s41284-023-00383-4.
[19] Muggah, R. (2023). Organized crime in armed conflicts and other situations of violence. *International Review of the Red Cross*, 105(923), 569-574. doi: 10.1017/S1816383123000036.
[20] Murashko, A.M. (2021). *Implementation of state policy in the fields of national security and defense at the regional level*. (PhD thesis. East Ukrainian National University named after Volodymyr Dahl, Severodonetsk, Ukraine).
[21] National Anti-Corruption Bureau of Ukraine. (2024). *Volyn customs criminal case: Suspects detained.* Retrieved from https://nabu.gov.ua/en/news/zlochinna-organ-zatc-ia-na-volins-k-i-mitnitc-10-p-dozriuvanikh/.
[22] National Police of Ukraine. (2023). *Results of the National Police's work: Arms dealers, arsenals, and ammunition stocks detected*. Retrieved from https://mvs.gov.ua/news/torgovci-zbrojeiu-sxroni-ta-arsenali-bojepripasiv-rezultati-roboti-nacpoliciyi-za-rik.
[23] Ofusori, A., & Hendradi, P. (2023). The impact of Dark Web markets on organized crime: Monitoring and enforcement challenges. *International Journal of Information Security and Management*, 12(2), 101-123. doi: 10.1234/ijism.2023.01234.
[24] Pardal, M., Eekelschot, L., Hoorens, S., & Blondes, E.L. (2023). *Insights into the effectiveness of preventive instruments in tackling organised crime: Summary*. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2303-1/RAND_RRA2303-1.summary-English.pdf.
[25] Roks, R., Bisschop, L., & Staring, R. (2021). Getting a foot in the door: Spaces of cocaine trafficking in the port of Rotterdam. *Trends in Organized Crime*, 24(2), 171-188. doi: 10.1007/s12117-020-09394-8.
[26] Travaglino, G.A., Abrams, D., Russo, G., & Gattino, S. (2023). Naming the threat: Lay prototypes of organized crime in Italy. *Psychology, Crime & Law*, 29(4), 417-437. doi: 10.1080/1068316X.2023.2239425.

Перспективи впровадження європейського досвіду боротьби з організованою злочинністю в Україні: теоретико-управлінські та правові засади державного регулювання у сфері національної безпеки

Олексій Копан
Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-0797-7952
Владислав Мельник
Кандидат юридичних наук, доцент
Інститут наукових досліджень з цивільного захисту
Національного університету цивільного захисту України
02000, вул. Вишгородська, 21, м. Київ, Україна
https://orcid.org/0000-0002-2659-9942

Анотація
Статтю присвячено аналізу сучасних підходів до боротьби з організованою злочинністю. Акцентовано на забезпеченні стійкості системи безпеки. Визначено ключові елементи стійкості, адаптивні механізми та стратегічні пріоритети в умовах трансформаційних загроз. Досліджено інтеграцію концепції стійкості в державну кримінальну політику та міжнародну взаємодію. Метою статті є вивчення теоретико-правових та управлінських засад імплементації європейського досвіду боротьби з організованою злочинністю в Україні крізь призму забезпечення стійкості національної безпеки. Методологічну основу дослідження становили формально-логічний, системний, порівняльно-правовий аналіз, а також методи контент-аналізу міжнародних стратегічних документів і статистичних даних. У дослідженні узагальнено підходи провідних європейських країн до протидії організованій злочинності, визначено ключові напрями адаптації цього досвіду в умовах сучасних викликів і загроз. Посилену увагу зосереджено на ролі інституцій ЄС у формуванні політики у сфері безпеки та можливостям їх інтеграції у правову систему України. Це надало можливість з'ясувати особливості європейських моделей запобігання та протидії злочинним організаціям, їхню взаємодію з державними та громадськими інституціями, а також механізми забезпечення стійкості системи безпеки. Підтверджено, що ефективна протидія організованій злочинності потребує поєднання правових, управлінських, технологічних і соціальних інструментів. Встановлено, що інтеграція досвіду ЄС в українське законодавство є можливою за умови гармонізації нормативно-правової бази, упровадження сучасних цифрових технологій у сферу кримінальної аналітики, а також підвищення рівня міжвідомчої координації. Сформовано концепцію «стійкої системи безпеки» як адаптивного інституту, здатного ефективно реагувати на транснаціональні загрози та гібридні виклики. Практична значущість полягає в розробленні пропозицій щодо інтеграції територіальної оборони в архітектуру національної безпеки України та впровадження європейських стандартів у національне законодавство

Ключові слова:
стійкість системи безпеки; організована злочинність; національна безпека; європейський досвід; територіальна оборона; правове регулювання

UDC 343.98:343.352
DOI: 10.63341/naia-chasopis/2.2026.18

ISSN 2519-4216
E-ISSN 2519-4313

Legal and practical aspects of the application of OSINT methodologies for evidence collection during pre-trial investigation of public office offences

Oleksandr Amelin*
PhD in Law, Associate Professor
Office of the Prosecutor General
01011, 13/15 Riznytska Str., Kyiv, Ukraine
Educational and Scientific Institute of Law of State Tax University
08201, 31 Universytetska Str., Irpin, Ukraine
https://orcid.org/0000-0002-0933-2111

Abstract
The purpose of the study was to examine legal constraints, procedural requirements, and practical challenges arising during the recording, verification, and use of information from open sources in proceedings concerning public office offences. Contextual, legal and regulatory, and problem-oriented analysis methods were employed to achieve the purpose. Given the increasing trend in the number of such offences in 2024-2025, the use of information from open sources is appropriate for the timely identification of criminal schemes, prevention of losses, and strengthening of public trust in state institutions. The study drew on an examination of the regulatory framework and contextual analysis to identify strengths and prospects of evidence collection from open sources, including broad access to relevant information, rapid data acquisition, and the possibility of investigating offences across different segments of state activity, including military, educational, medical, and other domains. The analysis found a number of problems and risks with using open-source information, such as the lack of standard procedures, limited technical skills, and possible ethical issues. Examination of these challenges informed recommendations aimed at improving the effectiveness of using open sources in the investigation of public office offences. Improvement of investigative effectiveness involved transformation across multiple dimensions, particularly regulatory, procedural, institutional, staffing, methodological, technical, ethical, and control-related aspects. The results of the study may be used by legislators to improve the regulatory framework, by law enforcement bodies and investigators to enhance the effectiveness and quality of investigations into public office offences, by researchers for further analysis of methodologies for processing information from open sources, and by educational institutions for the development of training programmes and courses on the use of digital evidence in criminal proceedings

Keywords:
open-source information; personal data; declarations; registers; disinformation; deepfakes; illicit enrichment

Article's History:
Received: 18.12.2025
Revised: 26.03.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Amelin, O. (2026). Legal and practical aspects of the application of OSINT methodologies for evidence collection during pre-trial investigation of public office offences. *Law Journal of the National Academy of Internal Affairs*, 16(2), 18-30. doi: 10.63341/naia-chasopis/2.2026.18.

*Corresponding author (*yuamelinoleksandr@gmail.com*)

Introduction

The importance of analysing the legal and practical dimensions of implementing Open Source Intelligence (OSINT) methodologies in the pre-trial investigation of public office offences is underscored by the digitalisation of social interactions and the increasing significance of open information resources in public administration. When someone commits a crime while in public office, they leave digital traces in open state registers, electronic declarations, public procurement systems, social media, and other online platforms. This makes it easier to find them. The lack of clear regulatory recognition of OSINT as a separate tool in the Criminal Procedure Code of Ukraine, the uncertainty surrounding the evaluation of the admissibility and evidentiary value of results derived from open-source analysis, and the potential for infringing on human rights and freedoms necessitate a thorough academic investigation into the legal parameters and practical application of OSINT in the operations of pre-trial investigation entities.

The potential for OSINT methodologies in criminal investigations is evidenced in academic literature, notably the research conducted by S. Bocharov *et al.* (2025). These researchers highlighted the validity of utilising information from open sources, including social media, government registries, mass media, and satellite imagery, for criminal investigations. According to S. Bocharov *et al*., the effectiveness of OSINT methodologies increases through integration with other intelligence disciplines, namely Human Intelligence, Signals Intelligence, and Imagery Intelligence. Drawing on a review of thematic studies, academic literature, and industry reports, R. Sazibur (2025) examined the application of OSINT in threat detection, incident response, and forensic investigations. The researcher concluded that the use of OSINT methodologies improved threat detection, reduced the risk of data breaches, and increased analytical effectiveness. N. Breuer (2025) investigated the use of OSINT technologies to obtain data from an Italian pre-trial detention order and to analyse the Italian business register for the construction of networks representing the "Ndrangheta" group involved in infiltration into the legal business sector. The researcher concluded that OSINT offers several advantages over conventional closed sources, as it functions as a proxy for analysing local network structures. S. Szymoniak & K. Foks (2024) examined the advantages of using OSINT technologies in a case of the Federal Bureau of Investigation involving a woman who participated in mass protests in Philadelphia in 2020 and prepared criminal offences, including phishing attacks. The evidence obtained in that case indicated that the use of OSINT methodologies supports effective verification of the accuracy and reliability of information for objective investigation. O.Yu. Amelin *et al*. (2025) analysed the possibilities for implementing international experience in investigating criminal offences in the sphere of official activity to assess its applicability to the legal system of Ukraine. These researchers said that some analytical tools are okay to use, but their effectiveness depends on things like the independence of investigative bodies, clear jurisdiction, and openness of evidentiary procedures.

Challenges associated with the use of OSINT methodologies in criminal investigations have also been addressed previously, in particular by J. Rajamaki *et al*. (2022). The researchers examined the use of OSINT technologies in the context of investigating cases of child abuse. J. Rajamaki *et al*. concluded that a barrier to the use of the OSINT approach lies in procedures related to data storage for further investigation, since the fact of abuse cannot be documented or examined by anyone other than a law enforcement officer specifically assigned and trained for this purpose. Similar barriers were identified by B.S. Kosokhatko (2025), who focused on the use of OSINT methodologies in the investigation of war crimes committed by the Russian Federation against Ukraine. The researcher identified a gap concerning the procedural status of OSINT specialists in criminal investigations in Ukraine. This gap arises because, despite the importance of expertise required for collecting and analysing open-source data, the Criminal Procedural Code of Ukraine[1] does not recognise the opinion of a specialist as an official source; therefore, this legal inconsistency constrains the use of OSINT methodologies in criminal investigations. Ethical aspects of the use of OSINT technologies were analysed by M. Van der Woude & G. Torres (2024), who considered the use of open sources in journalistic investigations in the Netherlands. Interview results indicated that participants involved in investigations relied to a significant extent on personal judgement and continuous dialogue with colleagues when making decisions regarding confidentiality, which raises concerns about the objectivity of conclusions.

Analysis of previous studies indicates that, despite extensive examination of the potential of OSINT methodologies in criminal investigations, several issues remain unresolved. One such gap is the lack of a systematic account of the specific features of applying OSINT technologies in pre-trial investigations of public office offences. There is also a lack of systematic research on the procedural status of OSINT analysis results as evidence in criminal proceedings in Ukraine, particularly with regard to the requirements of admissibility, relevance, and reliability. In this context, the purpose of the study is to examine the legal and practical problems associated with the use of OSINT methodologies for evidence collection during the pre-trial investigation of public office offences. The objectives of the study are

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.

to analyse the legal grounds and procedural possibilities for the use of OSINT methodologies in pre-trial investigations of such offences, to identify key practical challenges and risks associated with the use of OSINT in investigative activities, and to propose directions for improving national legislation and investigative practice with reference to international experience in the use of OSINT methodologies.

Materials and Methods

To achieve the purpose of the study, contextual analysis was applied to identify trends in the commission and investigation of public office offences in 2024 and throughout 2025. The selection of this period reflects changes in law enforcement practice and statistical indicators of such offences under conditions of martial law and institutional transformations of law enforcement and anti-corruption bodies, as evidenced by official statistical data for the respective periods. Materials for the contextual analysis included official reports of the National Anti-Corruption Bureau of Ukraine (2024a; 2024b; 2025a; 2025b) and the Specialised Anti-Corruption Prosecutor's Office for the first half of 2024, the annual report for 2024, and reporting materials for the first half of 2025, which were used to generalise statistical indicators relating to the registration, investigation, and procedural progress of criminal proceedings concerning public office offences. The contextual analysis considered indicators such as the number of initiated pre-trial investigations, notices of suspicion, indictments submitted to court, as well as the amounts of funds recovered for the state and the value of prevented financial losses resulting from the detection of such offences during 2024-2025. Given the digitalisation of the evidentiary base in proceedings concerning public office offences, the methodological approach also encompassed an analysis of regulatory and methodological documents governing the recording, collection, and preservation of electronic (digital) evidence, particularly in the context of OSINT use.

The task of the legal and regulatory analysis consisted in examining the legal grounds for the use of OSINT methodologies in the pre-trial investigation of public office offences. The analysis was based on the following regulations: the Constitution of Ukraine[1], Criminal Code of Ukraine[2], Law of Ukraine No. 2297-VI "On Personal Data Protection"[3], Law of Ukraine No. 2135-XII "On Operational and Investigative Activities"[4]. These legal instruments were examined in terms of their content and key provisions, as well as their role in enabling the use of OSINT methodologies in pre-trial investigations of such offences. The classification of public office offences presented in this study was developed based on the Criminal Code of Ukraine and features the following articles: 364, 364-1, 365, 366, 367, 368, 368-3, 368-5, 369, 369-2, and 370. This framework lists the name of each crime, what it means, and how it relates to the use of OSINT.

The study utilised SWOT analysis to evaluate the practical implications of employing OSINT technologies in the investigation of public office offences. The recognised benefits and obstacles of OSINT utilisation were categorised through thematic grouping and allocated to the classifications S, W, O, and T, reflecting the internal attributes of the technologies, such as functional capabilities and constraints, as well as the external circumstances of their implementation, encompassing legal, institutional, and practical considerations. The results were checked for consistency by comparing them to other sources and doing the analysis again. Legal, technical, and ethical aspects of the use of open sources in the investigation of such offences were examined using the example of a case involving a judge suspected of illicit enrichment and submission of false declarations. In this instance, open digital data, specifically electronic declarations, open property registers, market listings, and related sources, were used as part of the evidentiary base to establish discrepancies between income and assets (Ukrinfopress, 2025).

The study applied a problem-oriented analysis, which involved step-by-step identification of key challenges associated with the use of OSINT technologies in the investigation of public office offences based on previously analysed material. Based on the synthesis of identified challenges, recommendations were developed for improving OSINT strategies, including the identification of responsible actors for implementation and metrics for evaluating effectiveness, with consideration of legal, technical, and ethical constraints associated with the application of such technologies.

Results

Legal basis for the use of OSINT methodologies in pre-trial investigation

In this study, public office offences are defined as criminal offences committed by a public official in the course of, or in connection with, the exercise of official duties, through the use of granted authority or official position (Amelin, 2024). The study indicates that Articles 364-370 of the Criminal Code of Ukraine define, in different ways, practical scenarios for the use of OSINT methodologies in the investigation of public office offences. For offences related to abuse of power and authority

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text.
[4] Law of Ukraine No. 2135-XII "On Operational and Investigative Activities". (1992, February). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2135-12?lang=en#Text.

(Articles 364, 364-1, 365 of the Criminal Code of Ukraine), OSINT is used primarily for the analysis of open data on managerial decisions, public procurement, corporate linkages, and digital traces of official activity. For cases of official forgery and negligence (Articles 366 and 367 of the Criminal Code of Ukraine), open sources are used to check the accuracy of official documents and find differences between public records and what actually happened. Corruption offences related to undue advantage and bribery (Articles 368, 368-3, 369, 369-2 of the Criminal Code of Ukraine) are characterised by the use of OSINT to establish links between benefits, official decisions, and socio-economic relationships of the actors involved. The highest evidentiary relevance of OSINT arises in cases of illicit enrichment (Article 368-5 of the Criminal Code of Ukraine), where open digital sources enable the identification of inconsistencies between income and assets. At the same time, in proceedings under Article 370 of the Criminal Code of Ukraine, the use of OSINT remains limited due to the prohibition of provocation of bribery.

Conclusions regarding the dynamics of public office offences were drawn based on reporting materials of the National Anti-Corruption Bureau of Ukraine (2024b; 2025a) and the Specialised Anti-Corruption Prosecutor's Office. According to data for 2024-2025, during this period detectives of the National Anti-Corruption Bureau of Ukraine, in cooperation with prosecutors of the Specialised Anti-Corruption Prosecutor's Office, notified 115 individuals of suspicion in cases related to high-level corruption and public office offences, and submitted 69 indictments to court concerning 154 individuals out of a total of 370 initiated investigations, which is nearly twice the figure recorded in the first half of 2024. This comparison of quantitative indicators over time demonstrates a substantial increase in the activity of law enforcement bodies in the investigation of public office offences in 2025 compared with the previous year, which may be associated both with an increasing number of offences involving high-ranking officials and with procedural or institutional changes in the operation of the National Anti-Corruption Bureau of Ukraine and the Specialised Anti-Corruption Prosecutor's Office. The reporting period is also characterised by the exposure, for the first time in the history of the National Anti-Corruption Bureau of Ukraine and the Specialised Anti-Corruption Prosecutor's Office, of a sitting Deputy Prime Minister. During the same period, two corruption schemes within the Ministry of Defence were uncovered, with a total value of 733 million hryvnias. The reported data also indicate that in the first half of 2025, the National Anti-Corruption Bureau of Ukraine initiated 370 investigations and submitted 69 indictments to court concerning official offences. These figures emphasise that the problem of public office offences in Ukraine remains unresolved and requires attention already at the stage of investigation. The investigation of public office offences can be strengthened through the use of OSINT methodologies, which, although based on the analysis of open-source data, remain subject to specific legal provisions, as presented in Table 1.

Table 1. Legal grounds for the use of OSINT in pre-trial investigations

Regulation/source	Content/provisions	Role in the use of OSINT
Constitution of Ukraine (Articles 31, 32, 34)	Guarantees of the right to privacy, protection of personal data, secrecy of correspondence, and non-interference in private life; principle of openness of information	Defines the balance between the protection of privacy and the collection of open-source information for evidentiary purposes
Criminal Procedure Code of Ukraine (Articles 87, 89, 94)	Defines the procedure for the collection of evidence, including documents, public sources, and other factual information	Permits the lawful documentation and use of information from open sources as evidence
Law of Ukraine "On Personal Data Protection"	Regulates the procedure for the processing of personal data, including data obtained from open sources; establishes the principles of legality, proportionality, and minimisation	Restricts and directs the use of OSINT in relation to the collection and analysis of personal data
Law of Ukraine "On Operational and Investigative Activities"	Defines the procedure for the application of overt and covert investigative and counterintelligence measures conducted through the use of operational and operational-technical means	Plays an important role in distinguishing between OSINT and covert measures, particularly during the use of specialised software tools

Source: compiled based on Law of Ukraine No. 2135-XII "On Operational and Investigative Activities"[1], Constitution of Ukraine[2], Law of Ukraine No. 2297-VI "On Personal Data Protection"[3]

The presented table demonstrates that the use of OSINT methodologies in pre-trial investigation in Ukraine is grounded in a set of regulations that cover constitutional guarantees, procedural provisions,

[1] Law of Ukraine No. 2135-XII "On Operational and Investigative Activities". (1992, February). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2135-12?lang=en#Text.
[2] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[3] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text.

legislation on information, and personal data protection. The Constitution of Ukraine establishes fundamental principles of privacy protection and confidentiality of personal life, while also securing the right of access to open information, which forms the legal basis for the lawful collection of data from open sources. Law of Ukraine No. 2657-XII "On Information"[1] and Law of Ukraine No. 2297-VI "On Personal Data Protection"[2] further specify the framework for the use of open information and personal data. The former regulates access to information and distinguishes between open and restricted information, thereby providing legitimacy for OSINT methodologies when operating with open sources. The Law of Ukraine No. 2297-VI "On Personal Data Protection" emphasises the need to limit the processing of personal data and to comply with the principles of proportionality and minimisation of interference, which is critical for preventing violations of individual rights and ensuring the admissibility of evidence in court.

Practical challenges and risks of applying OSINT methodologies

The conducted SWOT analysis identifies key external and internal factors that influence the effectiveness of applying OSINT methodologies in the pre-trial investigation of public office offences in Ukraine; the results are presented in Table 2. OSINT methodologies in Ukraine have internal strengths, including rapid access to open sources and the ability to collect evidence in a timely manner. Nevertheless, weaknesses are present, including the lack of standardised procedures, limited technical resources, and a shortage of qualified analysts. Opportunities include the use of OSINT for documenting war-related and corruption offences and the development of international cooperation, while threats include the risk of disinformation, violations of privacy, and the potential legal inadmissibility of evidence. Effective use of OSINT therefore requires a combination of technical, methodological, and legal measures that maximise advantages and minimise associated risks.

Table 2. SWOT analysis of the application of OSINT methodologies in the investigation of public office offences in Ukraine

Component	Internal factors	External factors
Strengths	Speed of data collection and verification: the OSINT analysis of declarations and open registers assisted the National Anti-Corruption Bureau of Ukraine in identifying corruption schemes involving illicit enrichment and the embezzlement of assets (for example, cases concerning the illicit enrichment of members of parliament and high-ranking officials, where declaration data differed substantially from actual assets)	Establishment of judicial practice: the Supreme Court of Ukraine confirms the admissibility of electronic evidence when properly documented, which permits the inclusion of OSINT data in cases concerning corruption and public office offences
Weaknesses	Absence of standardised protocols: in several proceedings, detectives of the National Anti-Corruption Bureau of Ukraine encountered situations in which data from open sources were declared inadmissible because of improper documentation, which complicated the advancement of particular proceedings before the High Anti-Corruption Court	Inconsistency in judicial approaches: certain courts impose increased requirements concerning metadata and the methods used for documenting OSINT data, which complicates their use in cases concerning public office offences (for example, cases involving evidence related to embezzlement schemes in the defence sector)
Opportunities	Integration of OSINT into investigative algorithms: in major proceedings, such as the exposure of schemes involving the embezzlement of food supplies for the defence sector or fraud related to land rights during Operation "Clean City" conducted by the National Anti-Corruption Bureau of Ukraine, OSINT enabled the rapid identification of networks of individuals and the connections between them during the early stages of investigations	International harmonisation: the use of the practice of the European Court of Human Rights concerning digital evidence and the positions of the Supreme Court of Ukraine contributes to strengthening the evidentiary value of OSINT in cases concerning public office offences
Threats	Incorrect interpretation of data: without appropriate analytical training, OSINT conclusions may be interpreted incorrectly, which leads to delays in investigations or the exclusion of data from proceedings	Recognition of evidence as inadmissible: strict requirements concerning procedural documentation and privacy rights may result in the rejection of OSINT materials in court, and practice has demonstrated such situations in particular episodes of corruption investigations involving officials participating in large-scale schemes

Source: compiled based on C. Adionyi (2024), S. Lehominova *et al.* (2024), National Anti-Corruption Bureau of Ukraine (2024a; 2024b), A. Yadav *et al.* (2023), M.J. Yuthvek *et al.* (2024)

The analysis provides a basis for conclusions regarding the advantages and prospects of using OSINT technologies in the investigation and prevention of public office offences. According to the press service of the Specialised Anti-Corruption Prosecutor's Office, a judge of one of the courts in Kyiv acquired assets whose value exceeded his lawful income by more than 16 million UAH, while declarations contained inaccurate information regarding owned property and its valuation, which formed the basis for notification of

[1] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[2] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text.

suspicion under Article 368-5 and Part 2 of Article 366-2 of the Criminal Code of Ukraine, namely illicit enrichment and declaration of false information (Ukrinfopress, 2025). This case is illustrative, as conventional mechanisms of control over declarations and financial reporting often do not allow the identification of concealed assets or discrepancies between declared data and actual circumstances without the use of additional analytical methods. In this context, OSINT technologies significantly expand investigative capabilities through the systematic collection, verification, and analysis of large volumes of data from public registers, social media, open databases, and other accessible sources, which enables identification of undisclosed assets, establishment of network relationships between individuals and property, and development of digital evidence applicable in criminal proceedings concerning public office offences, which is supported by contemporary OSINT research indicating that the development of methodologies and automated tools increases the efficiency and accuracy of open-source data analysis, making OSINT an important element of modern intelligence practice (Ivkova & Opirskyy, 2025). Legal positions of the Supreme Court of Ukraine (2024; 2025), set out in decisions of 2024-2025 concerning admissibility, relevance, and evaluation of digital evidence and information from open sources in criminal proceedings on public office offences, indicate the gradual development of judicial practice that recognises the evidentiary value of open-source data subject to compliance with procedures of verification and assessment, which expands the prospects for wider use of OSINT in such investigations and strengthens the evidentiary base, increasing the effectiveness of anti-corruption proceedings.

Improvement of the effectiveness of OSINT methodologies in the investigation of public office offences occurs through systematic analysis of problems and risks, followed by the development of procedures and response strategies. One of the key practical challenges is the identification, verification, and proper documentation of reliable information within large volumes of open data, which is essential for establishing facts that may influence the course of criminal proceedings and the legal liability of public officials (National School of Judges of Ukraine, 2025). For example, OSINT data from electronic declarations, property registers, or public procurement systems are used to confirm discrepancies between declared income and actual assets in proceedings concerning illicit enrichment and abuse of power, particularly through integrated analysis of declarations and digital traces, and these approaches are described as key practical elements in the analysis of open sources in legal research and practice. Law enforcement and the judicial system in Ukraine are also improving their skills and knowledge about OSINT. For example, they are holding seminars and webinars for judges and investigators on the best ways to collect, verify, and document digital evidence, including how to present OSINT data as part of electronic evidence in criminal cases. These kinds of projects are meant to make the use of open sources in real investigations of public office crimes, like corruption cases involving abuse of office or illegal enrichment, better. For example, courts need proper recording, validation, and legal justification of OSINT materials for them to be accepted.

Another practical problem is that there is too much open data because new digital tools and platforms are becoming more common. The Ukrainian Helsinki Human Rights Union (2021) says that the digital footprint keeps getting bigger, which makes it harder to analyse OSINT data when looking into crimes committed by public officials. Social media, forums, videos, open databases, and other sources create a constant stream of digital information that police and analysts must sort through, filter, and organise to find signs of crimes, such as abuse of power, overstepping authority, or getting an unfair advantage. When there is so much data, there is a real risk of evidentiary overload, where important information might be missed or misinterpreted because there aren't good ways to process and classify it all. This problem isn't just a problem during war; it also happens in criminal cases involving official actions, where it's important to tell the difference between useful digital traces and wrong or unimportant data. The Ukrainian Helsinki Human Rights Union's report also says that even big government agencies like the National Anti-Corruption Bureau of Ukraine and the Specialised Anti-Corruption Prosecutor's Office have trouble processing a lot of data, especially when it comes in different formats and contexts. To analyse big datasets from open sources, you need systems for storing, sorting, and processing them automatically. This includes software that lets you filter data in a structured way, find the right indicators, and make sense of the results. Without these tools, investigators might miss important digital clues or misread open data, which could lead to wrong conclusions in criminal cases involving public officials.

In addition to the challenges identified, there are also significant constraints on the available resources and competence to analyse open sources, especially due to the need to use more advanced platforms, software, geolocation, and satellite imagery in the process. Training programmes and courses on OSINT are in the initial stages of development in Ukraine, and the level of training varies. International courses and training programmes organised by the Council of Europe have focused on training prosecutors and investigators in the use of open sources in criminal investigations, including war crimes investigations (Council of Europe Office in Ukraine, 2022). Another international training of trainers' programme for academic institutions has aimed to train specialists in OSINT who will train law enforcement agents of Ukraine in the techniques

for verifying and analysing open-source information (Kharkiv National University of Internal Affairs, 2025). Basic online courses, such as the OSINT School on the Diia.Education platform offer training in searching for and verifying open-source data, geolocation, and the use of reverse image search techniques but do not include training on using that data in court proceedings. The difference in the focus of each of these training programmes accounts for the differences in the competence of practitioners in the field of OSINT.

Within the investigation of offences committed by public office, the issue of the protection of personal data of the individuals encountered within the open sources presents a problematic issue. Investigations based on open sources often require the analysis of content published to social media platforms, videos published online, and the geolocation data of the individuals in those videos to determine their involvement in the commission of the offences. Each of these data elements may contain personally-sensitive data about the individuals in those videos, such as their names, places of residence, contact information, photographs of themselves, or data regarding the relationships of those individuals to the members of their own families and their finances. In the lack of rules regarding the ethical use of such data, the information can be used against those individuals without a legal basis for such use, potentially leading to the violation of their human rights and the incorrect interpretation of the actions of the public officials involved in the offences. According to the Ukrainian Helsinki Human Rights Union (2021), while the open sources from which investigation of the public officials can be performed may contain information that is to be useful to the investigation, that information has the potential to be harmful to the rights of those individuals if it is incorrectly processed. For instance, social media platforms can be analysed to reveal the personal data of civilians who have little relation to the offences being investigated. Due to the lack of established standards for documenting open sources of evidence, as well as the analysis of such evidence in criminal cases, many courts and investigators are sceptical of the use of such information within criminal investigations (Radeiko, 2025). Furthermore, as H.-W. Huang *et al.* (2025) state in their publication on issues related to the investigation of public officials, open sources of digital data cannot be documented properly without the inclusion of features to record the metadata of that digital data, to cryptographically secure that data, and to document the digital data and its analysis in the reports of the investigators. Without such proper documentation, the digital data from open sources is often rejected as admissible in the courts, as has happened in the prosecutions of individuals in various international jurisdictions.

Considering the above, it is possible to conclude that the methodology of OSINT can be used in the investigation of offences committed by public office. The selection of the tools to be utilized in the investigation and the implementation of those tools indicates the challenges that might exist in the investigation of these types of crimes, such as the difficulty in accessing and reviewing the data, the need for ethical and impartial handling of the data, and the limited resources available to the police investigation itself. Understanding these challenges enables the development of appropriate responses and supports the planning of further use of OSINT technologies in the investigation of public office offences.

Improvement of the use of OSINT methodologies in pre-trial investigation of public office offences

The analysis of legal foundations and judicial practice and the SWOT assessment of the application of OSINT methodologies in pre-trial investigation of public office offences in Ukraine indicate the potential of this set of tools, while also identifying several systemic issues that reduce the effectiveness of its practical use. Key challenges include the absence of unified standards for the collection and documentation of OSINT data, risks of legal inadmissibility of digital evidence, a shortage of qualified analysts, overload of investigators with large volumes of open data, and risks related to violations of privacy and personal data protection. Recommendations aimed at addressing these challenges are systematised in Table 3.

Table 3. Support for the use of OSINT methodologies in the pre-trial investigation of public office offences

Area	Recommendation	Responsible entities	Performance metrics
Regulatory	Development of official methodological guidelines on OSINT	OPG, MIA, National Anti-Corruption Bureau of Ukraine	Existence of an approved document; number of proceedings referring to it
Procedural	Standardisation of requirements for documenting OSINT evidence	OPG, Supreme Court	Reduction in cases where evidence is declared inadmissible
Institutional	Establishment of specialised OSINT units	NABU, SBI, SSU	Number of units established; number of investigations conducted
Human resources	Systematic OSINT training for investigators	MIA, international partners	Number of trained specialists; assessment results
Methodological	Implementation of data verification standards	Law enforcement agencies	Share of verified data; reduction in erroneous conclusions
Technical	Procurement and deployment of analytical platforms	MIA, MDT	Data processing time; number of automated processes

Table 3, Continued

Area	Recommendation	Responsible entities	Performance metrics
Ethical	Development of an OSINT code of ethics	Ukrainian Parliament Commissioner for Human Rights	Number of complaints regarding privacy violations
Oversight	Prosecutorial supervision and judicial control over OSINT	Prosecutor's Office, courts	Quality of judicial reasoning regarding OSINT evidence

Note: MIA – Ministry of Internal Affairs; MDT – Ministry of Digital Transformation of Ukraine; OPG – Office of the Prosecutor General; SBI – State Bureau of Investigation; SSU – Security Service of Ukraine
Source: developed by the researcher

The analysis affirms that enhancing the application of OSINT methodologies in the pre-trial investigation of public office offences in Ukraine necessitates a holistic and systematic approach that addresses the legal, organisational, methodological, technical, and ethical aspects of investigative practices. There needs to be progress on both the legal and procedural fronts. The lack of specific rules in the Criminal Procedure Code of Ukraine and other laws about how to use OSINT makes it unclear whether such evidence is acceptable in court. It is therefore appropriate to develop and adopt unified departmental methodological guidelines for investigators and prosecutors. These guidelines should set the legal limits on how to gather information from open sources, what makes it valid as evidence, and what metadata needs to be recorded, including the source, time of acquisition, publication context, and preservation. Standardisation like this helps create consistent law enforcement practices and lowers the chance that digital evidence will be thrown out of court.

One important area is making law enforcement agencies better at open-source analysis. In practice, the use of OSINT is often assigned directly to investigators, who simultaneously conduct procedural actions and analytical processing of data, which leads to overload and reduced quality of analysis. Institutionalisation of OSINT analytics through the establishment of specialised units or inter-agency groups represents an effective approach, as research has indicated that the development and formalisation of OSINT methodologies increases the accuracy of collection and analysis of open data and establishes OSINT as a key element of modern intelligence and decision-making in the field of national security (Ivkova & Opirskyy, 2025). Within such a model, the investigator retains procedural responsibility for the use of information, while the analyst is responsible for its technical and analytical processing, which contributes to improving the quality of the evidentiary base in proceedings concerning public office offences.

The methodological dimension of the use of OSINT methodologies is also significant, as open sources are characterised by high levels of informational noise, disinformation, and manipulation. Minimisation of these risks requires the implementation of standardised approaches to assessing the reliability of information, including multi-level verification of data, analysis of the context of dissemination, and critical evaluation of sources; such approaches were described in international OSINT research as a critical component of fact verification and reduction of errors when working with open data, particularly within models of multi-dimensional truth verification and integration of contextual information (Wang *et al*., 2022). The documentation of the logic of the analytical conclusions that are made, the tools used in the analysis, and the methods of verifying the results of that analysis will become a mandatory element of OSINT investigations in order to ensure the transparency of the investigation's analytical processes.

The technical support of the OSINT analysis will be a priority task due to the growing volume of digital information and the increasing number of open digital platforms from which that information can be obtained, but which cannot be manually processed; automated software analysis tools will improve the accuracy of investigations into corrupt and professional connections, as well as reduce the amount of time that is required for those investigations to be performed. The implementation of secure systems for the storage of OSINT data with controlled access also remains important because such systems will contribute to the preservation of the confidentiality and integrity of information.

A separate set of recommendations concerns compliance with standards for the protection of personal data and the privacy of individuals whose information appears in open sources. Although OSINT methodologies rely on the analysis of publicly available information, this does not remove the obligation to adhere to the principles of legality, proportionality, and the minimisation of interference in private life. The use of open-source data without appropriate ethical and procedural safeguards may lead to unjustified interference with the rights of individuals who are not subjects of criminal proceedings and may call into question the legitimacy of the obtained evidence. For this reason, the development of internal ethical standards for the application of OSINT and the mandatory assessment of risks to human rights during large-scale digital investigations remain important, similarly to international ethical codes and practices that require respect for privacy, legality, and the minimisation of harm during work with open-source data, which is widely discussed

in academic research on OSINT and human rights, particularly in studies that examine the ethical limitations of OSINT and the necessity of regulation for the protection of human rights during the use of open-source data by E. Millett (2023).

Thus, the improvement of the use of OSINT methodologies in the pre-trial investigation of public office offences in Ukraine should occur through the combination of regulatory governance, institutional strengthening, methodological standardisation, technical modernisation, and adherence to ethical principles. The implementation of such a comprehensive approach will increase the effectiveness of the identification and documentation of official offences, ensure the admissibility of digital evidence in court, and strengthen public trust in the activities of law enforcement agencies under conditions of the digitalisation of criminal justice.

Discussion

The study examined the prospects for the use of data from open sources during the pre-trial investigation of public office offences. These prospects were identified through the analysis of the annual report of the National Anti-Corruption Bureau of Ukraine and the SWOT analysis. The conclusions regarding the application of OSINT methodologies in investigations received full or partial support in previous research, including the study conducted by J. Rajamaki & K. Tiitta (2024). After examining international financial organisations, J. Rajamaki & K. Tiitta concluded that the use of information from open sources was advisable for the timely identification and prevention of threats. A similar position appears in the present study, which emphasises that investigations conducted by the National Anti-Corruption Bureau of Ukraine exposed schemes within the Ministry of Defence amounting to 733 million hryvnias. The analysis nevertheless considered the different research focuses, because the study conducted by J. Rajamaki & K. Tiitta concentrated exclusively on the financial sector, whereas the present study examined public office offences that may produce not only financial consequences, but also broader forms of impact.

V. Bilous *et al.* (2024) supported the argument presented in this study that the use of information from open sources contributes to situational awareness and strategic planning. The present study considers this issue, in particular, through the case of a judge whose actual assets substantially exceeded declared income. Despite the similarities between the current study and the research of V. Bilous *et al.*, the research of the authors exclusively examined the use of OSINT methodologies within military contexts. In contrast, public office offences may emerge in a variety of contexts. The research of Z. Avrahami *et al*. (2025) investigated the use of OSINT methodologies in the context of cybersecurity threats to organisations. The researchers analysed the experiences of both public and private companies to determine that the use of OSINT methodologies enabled those organisations to identify and respond to cyber threats in a timely manner. Although there are similarities between the study of Z. Avrahami *et al.* and the present study, such similarities are only partial due to the different focuses of the two studies. Whereas Z. Avrahami *et al.* studied public and private organisations, the present study focused on public organisations. Furthermore, the argument of the present study that OSINT technologies can be applied to various sectors is supported by the study conducted by V. Scuro (2025). V. Scuro found that the use of information from open sources enables organisations to identify the individuals who have committed offences in the digital space, such as trafficking in cultural heritage. Though similar to the present study, the research of V. Scuro relates to the private sector only, whereas the majority of public office offences occur within the public sector. Nevertheless, the ability of OSINT methodologies to assist in the identification of and response to criminal activity was recognised in the comparison of the research of the present study to previous research studies on the topic.

Further analysis shows that, even though OSINT methods have a lot of benefits, using data from open sources also comes with a lot of risks and problems. The study of how OSINT methods are used in investigations of public office crimes found that it was hard to quickly and fairly analyse large amounts of open-source data. Similar conclusions appear in the study conducted by D. Van Puyvelde & F. Tabarez Rienzi (2025), who examined the widespread perception of OSINT technologies as a revolutionary approach to criminal investigations. The researchers noted that the exponential growth of data transforms the scale of intelligence activities and encourages both state and non-state actors to seek strategies for integrating OSINT methodologies and improving digital literacy. In the present study, this issue appears through the argument that one of the principal practical problems associated with the use of information from open sources is the high risk of disinformation, including the emergence of deepfakes. The study also argued that the possibility of falsifying information creates risks for individuals and legal entities that are not connected with the commission of public office offences. Issues concerning the protection of confidentiality during criminal investigations also appear in the study conducted by M. Konieczny & P. Wiecej (2025), who emphasised that the use of information from open sources involves a high risk of the unauthorised acquisition and misuse of personal data on the Internet. Unlike M. Konieczny & P. Wiecej, who opposed the use of OSINT methodologies in criminal investigations categorically, the present study supports a more moderate application of this technology. The idea of moderate application also appeared in the study conducted by G.P. Ramadhany (2024), who emphasised the potential of research based on open sources while stressing the

integration of such intelligence tools into the practice of law enforcement agencies. The proposed approaches to integration included the development of policies governing the application of OSINT methodologies, the training and retraining of specialists, and the strengthening of the material and technical resources available for investigations, strategies and recommendations that received full or partial reflection in the present study. The ethical application of OSINT methodologies also received attention in the study conducted by A. Koenig (2024), who emphasised that, regardless of the type of source used during an investigation, information should be collected and analysed in accordance with the principles of accuracy and respect for the dignity of the involved parties. This position fully corresponds with the recommendation presented in the present study concerning the development of a code of ethics for OSINT, the implementation of which could fall under the responsibility of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine. Thus, the emphasis placed in the present study on adherence to ethical standards during the use of open-source data received strong support in previous research concerning the application of OSINT methodologies.

The present study also examined the importance of interdisciplinary cooperation for the effective application of OSINT methodologies in investigations of public office offences. The effectiveness of such cooperation received more detailed consideration during the development of recommendations aimed at improving the effectiveness of the use of information from open sources. The importance of interdisciplinary cooperation during criminal investigations also received support in previous research, particularly in the study conducted by A. Mukhopadhyay *et al.* (2024), who examined interdisciplinary cooperation in the context of the continuously increasing volume of information. According to the researchers, the growing volume of data and the complexity of investigative tasks indicate the need to expand and accelerate OSINT investigations, including through crowdsourcing practices involving experts. Such an approach may improve the effectiveness of investigations within the national context, where distinctions exist between specialists and experts who possess different powers concerning the collection and interpretation of obtained data. The importance of interdisciplinary cooperation also appears in the study conducted by A. Karakikes & K. Kotis (2025), who analysed the prospects for the application of artificial intelligence tools in the analysis of open sources for the protection of state borders. The researchers assert that the execution of these strategies necessitates interdisciplinary collaboration among experts in machine learning, natural language processing, and computer vision. The comparison between the current study and the research by A. Karakikes & K. Kotis revealed only partial alignment, as the studies examined distinct forms of interdisciplinary cooperation: the current study focused on collaboration among law enforcement agencies, while their research concentrated on cooperation within the realm of computer technologies.

The identified correspondences underscore the significance of the current study and highlight the imperative for a more thorough investigation of the proposed issue. The present study contributes to academic discourse by delineating public office offences as a distinct category characterised by unique traits necessitating specialised investigative methodologies.

Conclusions

The study found that there was a trend toward more public office crimes. In the first half of 2025, the National Anti-Corruption Bureau of Ukraine informed 115 people of their suspicions in cases of high-level corruption. This is twice as many as the number reported in the previous reporting period. The timely exposure of public office offences helps to prevent losses and strengthens public trust in state authorities. The investigation of public office offences benefits from the analysis of open-source information, a practice that has proven both advisable and effective across various contexts. In Ukraine, the use of OSINT technologies in the pre-trial investigation of public office offences is regulated by a range of regulations that grant data from open sources the status of admissible evidence, provided that such data are properly documented and impartially verified for authenticity.

The application of OSINT methodologies in the investigation of public office offences guarantees broad access to open sources and rapid data collection. The prospects of OSINT technologies include their use in the investigation of public office offences across different sectors, including the military, educational, and medical sectors, together with the development of a digital evidence base. The analysis of the prospects for the application of OSINT methodologies also considered their weaknesses, including the lack of standardised procedures and trained analysts, together with insufficient material and technical resources. The threats associated with the application of OSINT methodologies include disinformation, fake content, and violations of privacy. From a practical perspective, the obstacles to the application of OSINT technologies in criminal investigations include difficulties related to the identification and processing of reliable information within extensive volumes of open-source data, the overload of open-source information and the impossibility of its rapid processing, resource and competency limitations, and the necessity of adhering to the ethical principles of anonymity and confidentiality during investigations.

The identified problems require changes across several areas, namely the regulatory, procedural, institutional, personnel, methodological, technical, ethical, and supervisory dimensions. Changes in these areas

include the development of official methodological recommendations concerning the application of OSINT technologies, the unification of requirements for the documentation of evidence obtained from open sources, the establishment of specialised OSINT units and the organisation of systematic training programmes, the implementation of unified standards for the verification of obtained data, the development of a code for the ethical use of OSINT approaches, and the provision of prosecutorial supervision and judicial oversight regarding their application. The study proposed that such state institutions as the Office of the Prosecutor General, the Ministry of Internal Affairs of Ukraine, the Ministry of Digital Transformation of Ukraine, the National Anti-Corruption Bureau of Ukraine, the Supreme Court of Ukraine, the State Bureau of Investigation of Ukraine, and the Security Service of Ukraine should bear responsibility for the implementation of these recommendations. The study also developed metrics for evaluating the effectiveness of the proposed strategies, including the reduction in cases where evidence is declared inadmissible, the number of established units, the number of trained specialists, the proportion of verified data, the time required for data processing, the proportion of automated processes, and the number of complaints concerning violations of privacy.

Future studies should cover a broader sample of cases, incorporating materials from open sources beginning in 2020. The expansion of the sample will assist in tracing the dynamics of public office offences, the use of information from open sources during their investigation, and strategies aimed at increasing the effectiveness of such application.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Adionyi, C. (2024). Harnessing OSINT to enhance the investigation of economic crimes. *Journal of Anti-Corruption Law*, 8, 159-174.

[2] Amelin, O.Yu. (2024). Certain aspects of the appointment and replacement of a prosecutor in criminal proceedings on crimes in the sphere of official activities. *Rule of Law*, 56, 143-154. doi: 10.18524/2411-2054.2024.56.315691.

[3] Amelin, O.Yu., Pyniaha, R., Zaloznyi, R., Dmytrova, O., & Kryvoshlykov, S. (2025). Investigation of criminal offences in the field of official activity: Analysis of international experience and the possibility of its application in Ukraine. *International Annals of Criminology*, 63(4), 768-790. doi: 10.1017/cri.2025.10110.

[4] Avrahami, Z., Zwilling, M., & Hajaj, C. (2025). Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access*, 13, 154229-154250. doi: 10.1109/ACCESS.2025.3603868.

[5] Bilous, V., Bodnenko, D., Khokhlov, O., Lokaziuk, O., & Stadnik, I. (2024). Open source intelligence for war crime documentation. *CEUR Workshop Proceedings*, 3654, 368-375.

[6] Bocharov, S., Tyshchuk, V., & Bielai, S. (2025). Use of OSINT in operational and investigative activities: Tools and legal aspects. *State Security*, 1(5), 25-30. doi: 10.33405/2786-8613/2025/1/5/336692.

[7] Breuer, N. (2025). Testing the reliability of OSINT network data for investigating organized crime infiltration of legal-market businesses. *Global Crime*. doi: 10.1080/17440572.2025.2567277.

[8] Council of Europe Office in Ukraine. (2022). *The Council of Europe supports training on OSINT tools for prosecutors and investigators of Ukraine*. Retrieved from https://surl.li/zlwjwh.

[9] Huang, H.-W., Shih, C.-H., Li, C.-Yu., & Teng, H.-Yu. (2025). A blockchain-based framework for OSINT evidence collection and identification. *Future Internet*, 17(12), article number 551. doi: 10.3390/fi17120551.

[10] Ivkova, V.S., & Opirskyy, I.R. (2025). Research of existing OSINT tools and approaches in the context of personal and state information security. *Computer Systems and Networks*, 7(1), 143-159. doi: 10.23939/csn2025.01.143.

[11] Karakikes, A., & Kotis, K. (2025). AI-assisted OSINT/SOCMINT for sefeguarding boarders: A systematic review. *Information*, 16(12), article number 1095. doi: 10.3390/info16121095.

[12] Kharkiv National University of Internal Affairs. (2025). *EUAM experts launch OSINT training course for KhNUIA representatives*. Retrieved from https://univd.edu.ua/en/news/22784.

[13] Koenig, A. (2024). Ethical considerations for open-source investigations into international crimes. *AJIL Unbound*, 118, 45-50. doi: 10.1017/aju.2024.2.

[14] Konieczny, M., & Wiecej, P. (2025). Anti-OSINT methods ensuring protection of personal data in the context of cybercrime. *Annuals of the Administration and Law*, 1(25), 127-144. doi: 10.5604/01.3001.0055.1100.

[15] Kosokhatko, B.S. (2025). Problems of using open-source intelligence in the investigation of crimes committed within the framework of an international armed conflict. *Uzhhorod National University Herald. Series Law*, 3(88), 277-284. doi: 10.24144/2307-3322.2025.88.3.41.

[16] Lehominova, S., Shchavinsky, Yu.V., Rabchun, D., Zaporozhchenko, M., & Budzynskyi, O. (2024). The threats of OSINT tools and ways to mitigate the consequences of their application for the organization. *Cybersecurity Education Science Technique*, 1(25), 294-303. doi: 10.28925/2663-4023.2024.25.294303.
[17] Millett, E. (2023). *Open-source intelligence, armed conflict, and the rights to privacy and data protection*. doi: 10.58866/HQKE7327.
[18] Mukhopadhyay, A., Venkatagiri, S., & Luther, K. (2024). OSINT research studios: A flexible crowdsourcing framework to scale up open source intelligence investigations. *Proceedings of the American Association for Computing Machinery. Human-Computer Interaction*, 8(CSCW1), article number 105. doi: 10.1145/3637382.
[19] National Anti-Corruption Bureau of Ukraine. (2024a). *Steadfastness and efficiency: NABU and SAPO results in the first half of 2024*. Retrieved from https://surli.cc/hyntnx.
[20] National Anti-Corruption Bureau of Ukraine. (2024b). *The results of the first half of 2024 indicate that NABU and SAPO are reaching new heights in eradicating corruption: The latest high-profile cases involve former and current top officials committing corruption crimes here and now*. Retrieved from https://surl.li/chtjpa.
[21] National Anti-Corruption Bureau of Ukraine. (2025a). *The first half of 2025 was marked by a number of high-profile relations for NABU and SAPO, particularly in the defence, land, and medical sectors. As in previous periods, the emphasis was on exposing high-level corruption taking place in the context of full-scale aggression by the Russian Federation*. Retrieved from https://reports.nabu.gov.ua/investigations/.
[22] National Anti-Corruption Bureau of Ukraine. (2025b). *Report. II half of 2024*. Retrieved from https://nabu.gov.ua/site/assets/files/48751/zvit_2024_ii_ukr-1.pdf.
[23] National School of Judges of Ukraine. (2025). *Application of OSINT in judicial practice: From legal foundations to practical cases*. Retrieved from https://surl.li/ybbduc.
[24] Radeiko, R.I. (2025). Theoretical and legal framework for the admissibility of OSINT evidence from social networks: Procedural requirements and methodological approaches (case study No. 990/232/24). *Scientific Notes of Lviv University of Business and Law*, 45, 110-116. doi: 10.5281/zenodo.15648855.
[25] Rajamaki, J., Lahti, I., & Parviainen, J. (2022). OSINT on the dark web: Child abuse material investigations. *Information & Security*, 53(1), 21-32. doi: 10.11610/isij.5302.
[26] Rajamaki, J., & Tiitta, K. (2024). Implementation of OSINT for improving an international finance sector organization's cybersecurity. *International Conference on Cyber Warfare and Security*, 19(1), 612-616. doi: 10.34190/iccws.19.1.1977.
[27] Ramadhany, G.P. (2024). Open-source intelligence (OSINT) tools for law enforcement. *Endless: International Journal of Future Studies*, 7(3), 21-33.
[28] Sazibur, R. (2025). *The art of open source intelligence (OSINT): Addressing cybercrime, opportunities, and challenges*. doi: 10.2139/ssrn.5281845.
[29] Scuro, V. (2025). Open-source intelligence (OSINT) for researchers and practitioners. In E. Smith & S. Austin (Eds.), *Researching a rigged game: Digital approaches to tracing the illicit trade in cultural objects* (pp. 11-28). Cham: Springer. doi: 10.1007/978-3-032-02014-7_2.
[30] Supreme Court of Ukraine. (2024). *Supreme Court Judges discussed with experts the issue of admissibility of electronic evidence obtained from open sources*. Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/.
[31] Supreme Court of Ukraine. (2025). *OSINT as evidence in the investigation of war crimes: Representatives of the Supreme Court participated in a thematic seminar*. Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/1883443/.
[32] Szymoniak, S., & Foks, K. (2024). Open source intelligence opportunities and challenges – a review. *Advances in Science and Technology Research Journal*, 18(3), 123-139. doi: 10.12913/22998624/186036.
[33] Ukrinfopress. (2025). *Judge with millions in assets: SAPO exposed illegal; enrichment of over UAH 16 million*. Retrieved from https://ukrinfopress.com/2025/09/suddya-z-milyonnym-maynom-sap-vykryla-nezakonne-zbahachennya-na-ponad-16-mln-hrn-ukrinfopres.
[34] Ukrainian Helsinki Human Rights Union. (2021). *War and justice: How investigators can effectively use OSINT and what to do with "court" decisions in uncontrolled territories*. Retrieved from https://helsinki.org.ua/articles/viyna-ta-pravosuddia-iak-slidchym-efektyvno-vykorystovuvaty-osint-ta-shcho-robyty-iz-rishenniamy-sudiv-na-nepidkontrolnykh-terytoriiakh.
[35] Van Puyvelde, D., & Tabarez Rienzi, F. (2025). The rise of open-source intelligence. *European Journal of International Security*, 10(4), 530-544. doi: 10.1017/eis.2024.61.
[36] Van der Woude, M., & Torres, G. (2024). The ethics of open source investigations: Navigating privacy challenges in a gray zone information landscape. *Sage Journals*, 26(10), 2184-2202. doi: 10.1177/14648849241274104.
[37] Wang, H., Li, Ya., Huang, Zh., & Dou, Y. (2022). IMCI: Integrate multi-view contextual information for fact extraction and verification. *arXiv*. doi: 10.48550/arXiv.2208.14001.

[38] Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. *Artificial Intelligence Review*, 56, 12407-12438. doi: 10.1007/s10462-023-10454-y.
[39] Yuthvek, M.J., Adheena, S., Charithra, Y., & Kalaiselvi, K. (2024). Analyzing business crimes by implementing OSINT architecture. *Indian Journal of Natural Sciences*, 15(83), 72456-72464.

Правові та практичні аспекти застосування OSINT-методик для збору доказів під час досудового розслідування службових злочинів

Олександр Амелін
Кандидат юридичних наук, доцент
Офіс Генерального прокурора
01011, вул. Різницька, 13/15, м. Київ, Україна
Навчально-науковий інститут права Державного податкового університету
08201, вул. Університетська, 31, м. Ірпінь, Україна
https://orcid.org/0000-0002-0933-2111

Анотація
Мета дослідження полягала у вивченні правових обмежень, процедурних вимог і практичних проблем, що виникають під час фіксації, перевірки та використання відомостей з відкритих джерел у провадженнях про службові злочини. Для досягнення мети використовувалися методи контекстуального, нормативно-правового та проблемно-орієнтованого аналізу. З огляду на тенденцію до збільшення кількості службових злочинів у 2024–2025 роках, було зроблено висновок про доцільність використання інформації з відкритих джерел для своєчасного виявлення злочинних схем, уникнення збитків і підвищення рівня суспільної довіри до державних інститутів. На підставі дослідження нормативно-правової бази та контекстуального аналізу визначено позитивні аспекти й перспективи пошуку доказів у відкритих джерелах, зокрема широкий доступ до релевантної інформації та її швидкий збір, а також можливість розслідування злочинів у різних сегментах державної діяльності – військовому, освітньому, медичному тощо. Як недоліки й загрози використання відкритих джерел інформації виокремлено недостатність стандартизованих процедур, слабку матеріально-технічну базу, а також потенційне порушення етичних норм. Вивчення проблемних аспектів дало змогу розробити рекомендації щодо підвищення ефективності використання відкритих джерел у розслідуванні службових злочинів. Підвищення ефективності розслідування передбачає трансформаційні процеси в різних напрямах, зокрема нормативному, процесуальному, інституційному, кадровому, методичному, технічному, етичному, а також у напрямі контролю. Результати дослідження можуть бути використані законодавцями для вдосконалення нормативно-правової бази, правоохоронними органами й слідчими – для підвищення ефективності та якості розслідування службових злочинів, науковцями – для подальшого аналізу методик опрацювання інформації з відкритих джерел, а освітніми установами – для розробки навчальних програм і тренінгів із застосуванням цифрових доказів у практиці кримінального провадження

Ключові слова:
відкриті джерела інформації; персональні дані; декларації; реєстри; дезінформація; діпфейки; незаконне збагачення

UDC 343.9:316.77:355.40
DOI: 10.63341/naia-chasopis/2.2026.31

ISSN 2519-4216
E-ISSN 2519-4313

The relationship between russian propaganda and certain criminogenic processes in Ukraine

Vadym Kudinov*
PhD in Physical and Mathematical Sciences, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-5299-0590

Oleksandr Pakrysh
PhD in Technical Sciences, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-6420-5246

Yuliia Panimash
PhD in Pedagogical Sciences
Cherkasy Institute of Fire Safety named after the Heroes
of Chernobyl of the National University of Civil Defense of Ukraine
18034, 8 Onopriyenko St., Cherkasy, Ukraine
https://orcid.org/0000-0002-5337-6613

Abstract
The article examined the influence of russian information and psychological operations on the public consciousness of Ukrainians with the aim of provoking criminal offences. russian narratives were analysed on their intensity using the number of occurrences of the selected russian language words in the propaganda materials. The number of specific crimes was based on the statistics of the Office of the Prosecutor General of Ukraine. The study revealed that from 2013 to 2025, there were statistically significant co-movements in the number of propaganda materials devoted to certain russian information and political psychological operations and certain types of registered crimes in Ukraine. On the basis of the correlation analysis, assumptions were made regarding the influence of particular propaganda narratives on statistics for selected categories of criminal offences. The exploratory factor analysis revealed the existence of three distinct factors of informational and criminogenic influence, which combine the dynamics of russian propaganda narratives with the dynamics of indicators of criminal offences against the foundations of Ukraine's national security, statehood, defence capability and territorial integrity between 2013 and 2025. Establishing the presence of an influence exerted by russian propaganda on criminal offence statistics, as well as the factors determining

Article's History:
Received: 10.02.2026
Revised: 05.05.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Kudinov, V., Pakrysh, O. & Panimash Yu. (2026). The relationship between russian propaganda and certain criminogenic processes in Ukraine. *Law Journal of the National Academy of Internal Affairs*, 16(2), 31-41. doi: 10.63341/naia-chasopis/2.2026.31.

*Corresponding author (*kudinov_va@ukr.net*)

this influence, will make it possible to develop future strategies aimed at reducing the effectiveness of russian propaganda and lowering the crime rate

Keywords:
information and psychological operations; information narratives; criminal offences; crime situation; rank correlation; factor analysis

Introduction

As of 2026, five main domains of warfare are commonly distinguished: land, sea, air, space and the information environment, including cyberspace. In the information environment, information and psychological operations, hereinafter referred to as PSYOPs, are traditionally conducted during war in order to influence or mislead military opponents or the civilian population. russian PSYOPs justify and support the armed aggression and annexation of territories that the russian federation has carried out against Ukraine since 2014 and that escalated into a full-scale war in February 2022.

Many publications have examined the impact of russian information narratives on the public consciousness of Ukrainians, addressing a broad range of issues. In the study by O. Sviderska (2022), four levels are identified at which information warfare operates in Ukrainian realities, while the concept of information warfare is equated with deliberate criminal acts aimed at misinforming and demoralising the population and creating its "silent submission". The influence of russian propaganda on young people in the temporarily occupied territories of Ukraine is examined by S. Sidchenko *et al*. (2024). The impact of russian propaganda on social processes and state stability in Ukraine is considered by Y. Minenko (2023). N. Chaban *et al*. (2023) analyse the mechanisms through which russian narratives about Ukraine are constructed, as well as the factors that make them persuasive. The role of bots in spreading pro-russian messages on social media in order to form false public perceptions is examined by D. Geissler *et al*. (2023). The mechanisms of dissemination of russian narratives and their influence on the information environment during the war, together with the counter-narratives of pro-Ukrainian actors based on the use of social media platforms, are studied by R. Marigliano *et al*. (2024).

The analysis of social survey data presented by V. Kudinov *et al*. (2025), as well as the results of surveys of the Ukrainian population concerning perceptions of disinformation and information manipulation during the war presented by L. Alonso-Martín-Romo *et al*. (2023), show that russian propaganda generally fails to achieve its aim of influencing the public consciousness of Ukraine's population and its readiness for national resistance against russian aggression. Given that social surveys are conducted among broad sections of the population, whereas russian PSYOPs directly affect certain limited categories of citizens, survey data may be insensitive to the negative manifestations of russian propaganda's influence. At the same time, prolonged armed aggression leads to psychological fatigue among the population, a decline in social optimism and a loss of belief in the prospect of a better future for Ukraine, which "contributes to a lower level of critical thinking, the normalisation of the russian federation's aggressive policy and the perception of political concessions as inevitable" (Rudnieva & Malovana, 2026).

International experience of military conflicts shows that propaganda can dehumanise certain groups of the civilian population and lower psychological barriers to the commission of violent crimes (Rawnak, 2025). Military hostilities, reinforced by aggressive russian propaganda, have become powerful factors in the spread of numerous acts of unlawful conduct among certain sections of Ukraine's population. Such acts often undermine the foundations of Ukraine's national security and defence capability and fall under specific articles of the Criminal Code of Ukraine[1]. Criminal offences related to the armed aggression against Ukraine have been analysed in scholarly publications, including collaboration activities (Katorkin, 2024), aiding the aggressor state (Kuksiuk, 2026), justification of the russian federation's armed aggression against Ukraine and the glorification of its participants (Kopcha, 2025), as well as unauthorised absence from a military unit and desertion.

The above-mentioned scholarly studies repeatedly noted the existence of links between russian PSYOPs and manifestations of unlawful acts committed by individual citizens. They also analysed and generalised the characteristics of citizens who commit certain types of crimes provoked by military hostilities. However, no quantitative assessment of the strength of these links has been carried out. This study aimed to identify indicators of consistency between changes in the number of russianlanguage propaganda materials related to specific russian information and psychological operations and changes in the number of particular types of registered crimes in Ukraine from 2013 onwards. The statistical relationship between changes in the number of registered offences under a particular Article of the Criminal Code of Ukraine and changes in the number of russian-language anti-Ukrainian propaganda materials in russian media was formulated as the following statistical hypothesis:

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2341-14.

- null hypothesis (H_0): changes in the number of registered crimes are not related to changes in the number of russian-language propaganda materials;
- alternative hypothesis (H_1): changes in the number of registered crimes are statistically significantly related to changes in the number of russian-language propaganda materials.

Materials and Methods

The study examined the relationships between six quantitative indicators of russian narratives and 14 types of criminal offences. This gave rise to the assumption that hidden structural links exist between the dynamics of the dissemination of particular propaganda narratives and the dynamics of specific types of crime, and that these links can be represented through a system of common latent factors. This assumption can be formulated as another research hypothesis: indicators of the intensity of dissemination of particular russian propaganda narratives and indicators of specific types of crime share a common latent structure, which is manifested through a limited number of factors and reflects systemic relationships between information influence and criminogenic processes. To test this research hypothesis, the study analysed the main factors that determine the consistency of these changes. Establishing the presence of such factors will make it possible in future to identify targeted preventive measures aimed at reducing the effectiveness of russian propaganda and lowering the crime rate.

The dynamics of the intensity with which particular russian propaganda narratives were used were assessed through content analysis of the frequency with which selected russian-language terms and phrases appeared in the content of russian information and political television over specific time intervals, namely one-year periods, between 2013 and 2025. This methodological choice is explained by the fact that the dynamics of such frequencies fairly accurately reflect the relative intensity with which russian narratives were transmitted to particular groups of Ukraine's population. Strengthened state control over the russian information space contributed to a high degree of consistency between the narratives of state television, pro-Kremlin online media and a substantial part of the russian segment of Telegram. Studies indicate intensive content exchange between russian television, russian media and Telegram channels, as a result of which key Kremlin narratives are reproduced across all communication environments (Hanley & Durumeric, 2024). The methodological basis is also supported by statistical studies showing that approximately 11% of Ukraine's population consumed russian media with some regularity in 2024, while russian television enjoyed the highest level of trust among consumers, at 25% (Internews Network, 2024). At the same time, it is evident that estimates of the intensity with which russian narratives are transmitted, when determined solely on the basis of television, are fairly approximate and relative in nature. They indicate the direction of change, namely whether use increased or decreased, but they do not allow a precise assessment of the extent to which the use of a particular term in a russian propaganda narrative increased or decreased. This should be taken into account when selecting methods for the statistical analysis of these data.

The frequency with which selected terms and phrases appeared was determined using the online resource War of Words (2026). The terms and phrases selected for analysis identify some of the main narratives of russian PSYOPs (Zalkin *et al*., 2025). The search results for selected russian-language terms from propaganda narratives, beginning in 2013 and broken down by annual periods, are presented in Table 1.

Table 1. Search results for selected russian-language terms from the narratives

Year	Bandera*	TCR	Denazification	Demilitarisation	Capitulation	Novorossiya
2013	9	0	0	1	16	1
2014	290	0	0	17	81	552
2015	218	0	3	64	102	305
2016	196	0	3	14	74	107
2017	439	0	11	28	135	156
2018	486	0	4	49	187	113
2019	857	0	21	54	685	180
2020	345	0	9	28	262	54
2021	522	0	15	29	342	139
2022	1245	3	482	1486	1004	419
2023	827	49	152	541	705	517
2024	384	711	84	357	623	609
2025	363	854	110	543	1,005	379

Note: the term "Bandera*" makes it possible to cover the words "Bandera", "Banderite", "Banderites" and "Banderism"
Source: developed by the authors based on data from War of Words (2026)

The crime situation for the period from 2013 to 2025, broken down by year for selected articles of the Criminal Code of Ukraine and selected categories of crimes, was determined on the basis of the uni-

fied annual report on criminal offences published on the website of the Office of the Prosecutor General of Ukraine (2026). The following 14 types of crimes were selected for the study, some of which were grouped under several articles of the Criminal Code of Ukraine (Table 2). The numerical indicators used were the number of recorded criminal offences in the reporting period. These numbers represent the number of registered proceedings, not convictions, nor the number of persons involved. A single individual can appear multiple times in multiple cases. Indicators of crimes under Articles 335, 336 and 337 were merged into one, No. 11 in Table 2. These are all related to evasion of military duty. Criminal offences against the established procedure for military service, under Articles 402-435, are also presented as a single aggregated item, No. 13 in Table 2. More than 95% of this category consists of crimes under Articles 407 and 408. It should be noted that, beginning in 2022, Table 1.20 from the annual reporting of the Office of the Prosecutor General, entitled "Criminal offences against the established procedure for military service (military criminal offences)", was removed from the general reporting files, as of 2026. However, for 2022-2024, information on this category of crimes is available in publicly accessible archive files, links to which are provided in the study by D. Hladchenko (2025). The total number of registered crimes in this category for 2025 and the first quarter of 2026 can be easily calculated from the general reporting files published on the website of the Office of the Prosecutor General of Ukraine (2026). This made it possible to produce forecast estimates for crimes under Articles 407 and 408 of the Criminal Code of Ukraine for the relevant time intervals, which correlate with the data for the first ten months of 2025 (Tatarenko, 2026).

Table 2. Types of crimes analysed in the study

No.	Articles of the Criminal Code of Ukraine[1]	Type of crime
1	109	Actions aimed at the violent change or overthrow of the constitutional order or the seizure of state power
2	110	Encroachment on the territorial integrity and inviolability of Ukraine
3	110-2	Financing actions committed to violently change or overthrow the constitutional order, seizing state power, or changing the borders of the territory or state border of Ukraine
4	111	High treason
5	111-1	Collaboration activities
6	111-2	Aiding the aggressor state
7	113	Sabotage
8	114	Espionage
9	114-1	Obstruction of the lawful activities of the Armed Forces of Ukraine and other military formations
10	332	Illegal transportation of persons across the state border of Ukraine
11	335, 336, 337	Evasion of conscription for compulsory military service or military service by conscription of officers (335) Evasion of conscription during mobilisation (336) Evasion of military registration or special training assemblies (337)
12	338	Desecration of state symbols
13	402-435	Criminal offences against the established procedure for military service, including: Unauthorised absence from a military unit or place of service (407) Desertion (408)
14	436-2	Justification, recognition as lawful or denial of the armed aggression of the russian federation against Ukraine, and glorification of its participants

Source: developed by the authors

Thus, the analysis included six dynamic interval series for the period from 2013 to 2025, with a one-year interval, containing the frequencies with which selected terms characteristic of russian narratives appeared, and 14 dynamic interval series for the same period, corresponding to changes in statistical indicators for particular types of criminal offences. In total, 20 dynamic interval series were obtained, each containing values for the relevant features, namely terms or crimes, over 13 annual periods. An intercorrelation matrix of 20 by 20 was calculated for these series, with each cell containing Spearman's rank correlation coefficient. On the basis of the resulting intercorrelation matrix, factor analysis was conducted using Principal Axis Factoring (PAF) with Varimax rotation. The number of factors was determined according to the Kaiser criterion, with eigenvalues greater than 1 selected. The statistical calculations for the individual elements of the intercorrelation matrix and the exploratory factor analysis were performed using ChatGPT (OpenAI, GPT-5.5, May 2026 version); all results obtained from the artificial intelligence were subsequently verified.

Although classical factor analysis involves the use of Pearson correlations, Spearman rank correlations are an acceptable robust non-parametric alternative

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2341-14.

when the data are not normally distributed (Goretzko & Bühner, 2022). In this context, the use of PAF is recommended (Qiu *et al.*, 2025), since it does not require multivariate normality, unlike methods based on Maximum Likelihood, which are sensitive to violations of normality.

Results

A fragment of the resulting intercorrelation matrix between changes in the frequency with which certain terms appeared and changes in criminal offences under specific articles is presented in Table 3. The obtained coefficient values indicate a noticeable rank correlation between many of the features under study. Since the number of annual periods from 2013 to 2025 is 13, the significance threshold for Spearman's rank correlation coefficient is 0.553 at a significance level of $\alpha = 0.5$ and 0.684 at a significance level of $\alpha = 0.1$.

Table 3. Rank correlation coefficients between the frequencies of occurrence of selected terms and statistical indicators for particular types of criminal offences

Articles of the Criminal Code of Ukraine	Bandera	TCR	Denazification	Demilitarisation	Capitulation	Novorossiya
109	0.6041	0.4616	0.5837	0.5304	0.64	0.5545
110	0.4451	0.7583	0.6336	**0.8226**	0.6758	**0.8022**
110-2	**0.8116**	**0.7527**	**0.9683**	**0.8402**	**0.9188**	0.5062
111	0.6374	**0.7516**	**0.8815**	**0.7538**	**0.8297**	0.4011
111-1	0.4765	**0.918**	**0.8143**	**0.7997**	**0.7382**	0.6577
111-2	0.4228	**0.9426**	**0.7873**	**0.7661**	**0.7114**	0.6845
113	0.1492	**0.7288**	0.4515	0.6777	0.5193	**0.7956**
114	**0.811**	**0.7547**	**0.8963**	**0.8232**	**0.8993**	0.6869
114-1	0.1568	**0.8199**	0.5738	**0.7149**	0.5915	**0.7895**
332	0.544	**0.812**	**0.7961**	0.674	**0.7967**	0.3462
335, 336, 337	0.3901	**0.765**	0.6198	**0.8446**	0.6319	**0.8297**
338	0.0607	0.2359	0.0553	0.3964	0.1297	0.5986
402-435	0.1923	**0.8187**	0.5813	**0.7428**	0.5769	**0.7527**
436-2	0.4765	**0.918**	**0.8143**	**0.7997**	**0.7382**	0.6577

Source: developed by the authors

Thus, in many cases, changes in the number of registered crimes under particular articles of the Criminal Code of Ukraine strongly correlate with changes in the intensity with which selected terms characteristic of certain russian narratives appeared. This may support the alternative hypothesis (H_1) formulated in the Introduction to this study. An analytical review of selected rows in Table 3 makes it possible to interpret the results of the rank correlation analysis as follows:

- Article 109 of the Criminal Code of Ukraine: actions aimed at the violent change or overthrow of the constitutional order. Moderate and high correlations were identified with all the terms examined (ρ = 0.46-0.64), with the highest values recorded for "Novorossiya" (ρ = 0.64), "Bandera" (ρ = 0.60) and "Demilitarisation" (ρ = 0.58). This may indicate that the dissemination of narratives concerning the supposedly artificial nature of Ukrainian statehood, the need for its "demilitarisation" and the creation of alternative political entities, such as "Novorossiya", may potentially contribute to the formation of anti-state attitudes associated with an increase in the number of offences under Article 109 of the Criminal Code of Ukraine.
- Article 110 of the Criminal Code of Ukraine: encroachment on the territorial integrity and inviolability of Ukraine. High correlations were observed with the terms "Capitulation" (ρ = 0.82), "Novorossiya" (ρ = 0.80), "Demilitarisation" (ρ = 0.76) and "Denazification" (ρ = 0.63). This result may indicate a link between the intensification of narratives concerning changes to Ukraine's state borders, the need for concessions to the aggressor, the legitimisation of russian territorial claims, and the dynamics of offences against the territorial integrity of the state.
- Article 110-2 of the Criminal Code of Ukraine: financing actions aimed at changing the boundaries of the territory or state border. Very high correlations were observed for most terms, especially "Denazification" (ρ = 0.97), "Novorossiya" (ρ = 0.92), "Capitulation" (ρ = 0.84) and "Demilitarisation" (ρ = 0.75). The results may indicate that the intensive dissemination of narratives aimed at justifying aggression and changing Ukraine's territorial order may be accompanied by increased activity among persons involved in financing such unlawful actions.
- Article 111 of the Criminal Code of Ukraine: high treason. The highest coefficients were observed for the terms "Denazification" (ρ = 0.88), "Novorossiya" (ρ = 0.83), "Demilitarisation" (ρ = 0.75) and "TCR" (ρ = 0.75). This may indicate that the dissemination of narratives which delegitimise the Ukrainian state and justify the actions of the aggressor state may potentially

create an information environment conducive to acts committed to the detriment of Ukraine's sovereignty and security.

- Article 111-1 of the Criminal Code of Ukraine: collaboration activities. Very high correlations were established with the terms "TCR" (ρ = 0.92), "Denazification" (ρ = 0.81), "Demilitarisation" (ρ = 0.80) and "Capitulation" (ρ = 0.74). This may indicate that the discrediting of Ukrainian institutions of government and defence, together with the dissemination of ideas concerning the need for concessions to the aggressor, may contribute to the formation of a tolerant attitude towards cooperation with representatives of the aggressor state.
- Article 111-2 of the Criminal Code of Ukraine: aiding the aggressor state. The correlation structure is similar to that for the previous article: the highest values were observed for "TCR" (ρ = 0.94), "Denazification" (ρ = 0.79), "Demilitarisation" (ρ = 0.77) and "Capitulation" (ρ = 0.71). This may indicate a possible link between the dissemination of narratives aimed at undermining trust in the Ukrainian state and the intensification of actions carried out in the interests of the aggressor state.
- Article 113 of the Criminal Code of Ukraine: sabotage. The highest coefficients were obtained for the terms "Capitulation" (ρ = 0.80), "TCR" (ρ = 0.73) and "Novorossiya" (ρ = 0.68). It may be assumed that the dissemination of narratives about the futility of resistance, the need for concessions and the legitimacy of russian geopolitical objectives may create an informational basis for sabotage activities.
- Article 114 of the Criminal Code of Ukraine: espionage. Very high correlation coefficients were observed for all the main terms (ρ = 0.69-0.90), with the highest values recorded for "Denazification" (ρ = 0.90), "Novorossiya" (ρ = 0.90), "Demilitarisation" (ρ = 0.82) and "Bandera" (ρ = 0.81). This may indicate that the active dissemination of propaganda narratives justifying russia's actions against Ukraine is associated with the dynamics of crimes aimed at collecting and transmitting information in favour of a foreign party.
- Article 114-1 of the Criminal Code of Ukraine: obstruction of the lawful activities of the Armed Forces of Ukraine and other military formations. The highest correlations were identified for the terms "TCR" (ρ = 0.82), "Capitulation" (ρ = 0.79) and "Demilitarisation" (ρ = 0.71). This may indicate that narratives aimed at discrediting mobilisation and the state's defence measures may be associated with an increase in cases of obstruction of the activities of the defence forces.
- Article 332 of the Criminal Code of Ukraine: illegal transportation of persons across the state border. High correlations were observed with the terms "TCR" (ρ = 0.81), "Denazification" (ρ = 0.80), "Novorossiya" (ρ = 0.80) and "Demilitarisation" (ρ = 0.67). One possible explanation is that campaigns aimed at discrediting mobilisation measures may encourage evasion of military duty and related attempts to cross the state border illegally.
- Articles 335-337 of the Criminal Code of Ukraine: evasion of conscription, military registration and training assemblies. The highest coefficients were obtained for the terms "Capitulation" (ρ = 0.83), "TCR" (ρ = 0.77), "Novorossiya" (ρ = 0.84) and "Demilitarisation" (ρ = 0.84). The results may indicate that the dissemination of narratives directed against mobilisation and the continuation of armed resistance potentially affects the increase in offences related to evasion of military duty.
- Article 338 of the Criminal Code of Ukraine: desecration of state symbols. For most terms, the correlation is weak or very weak (ρ = 0.06-0.40). A relatively moderate association is observed only for the term "Capitulation" (ρ = 0.60). This may indicate that the propaganda narratives examined have only a limited connection with the dynamics of this type of offence, and that its commission is probably determined by other factors.
- Articles 402-435 of the Criminal Code of Ukraine: military criminal offences. High correlations were identified with the terms "TCR" (ρ = 0.82), "Capitulation" (ρ = 0.75), "Demilitarisation" (ρ = 0.74) and "Novorossiya" (ρ = 0.75). This may indicate the possible influence of narratives that undermine motivation to serve, encourage unauthorised absence from the place of service and desertion, discredit military command, and call into question the expediency of continuing the defence of the state.
- Article 436-2 of the Criminal Code of Ukraine: justification, recognition as lawful or denial of the armed aggression of the russian federation against Ukraine. The highest coefficients were observed for the terms "TCR " (ρ = 0.92), "Denazification" (ρ = 0.81), "Demilitarisation" (ρ = 0.80) and "Capitulation" (ρ = 0.74). This is an expected result, since these terms belong to the key propaganda constructs used to justify aggression against Ukraine. High correlations may indicate a close relationship between the intensity with which such narratives are disseminated and the dynamics of offences under Article 436-2 of the Criminal Code of Ukraine.

The correlation analysis showed that the most stable predictors among the terms examined were "TCR", "Denazification", "Demilitarisation", "Capitulation" and "Novorossiya", which demonstrate high correlations with several groups of offences at once, including offences related to state security, collaboration activities, military criminal offences and the justification of the russian federation's aggression. This may be regarded as indirect confirmation of the criminogenic potential of the relevant russian information narratives. A strong correlation also exists between the frequencies of occurrence of the individual terms considered in this study, since they often appear simultaneously in the same russian information narratives. Similarly, a strong correlation is observed between the statistics for particular types of crimes. Taken together, these findings

suggest the existence of latent, or hidden, factors that simultaneously affect different types of criminal offences and the frequencies of occurrence of particular terms characteristic of russian narratives.

In view of the above, an exploratory factor analysis was conducted. It effectively demonstrated the existence of statistically linked latent factors between the dynamics of russian propaganda narratives and the dynamics of particular categories of criminal offences in Ukraine in 2013-2025. The exploratory factor analysis showed that the russian federation's information and propaganda campaigns, crimes against the foundations of Ukraine's national security, military criminal offences and mobilisation-related offences are not processes independent of russian information narratives. Rather, together with them, they form three stable latent factors, provisionally designated as F1, F2 and F3 and presented in Table 4.

Table 4. Factor loading matrix with Varimax rotation

No.	Terms/Articles of the Criminal Code of Ukraine[1]	F1	F2	F3
1	Bandera*	-0.0157	-0.0848	-0.9550
2	TCR	0.8844	-0.2993	-0.3237
3	Denazification	0.5327	-0.1045	-0.8040
4	Demilitarisation	0.5170	-0.4446	-0.5989
5	Capitulation	0.4571	-0.1991	-0.7920
6	Novorossiya	0.3939	-0.7458	-0.2496
7	Actions aimed at the violent change or overthrow of the constitutional order or the seizure of state power, Article 109	0.1492	-0.4553	-0.6186
8	Encroachment on the territorial integrity and inviolability of Ukraine, Article 110	0.4446	-0.7487	-0.4380
9	Financing actions committed to violently change or overthrow the constitutional order, or seizing state power, or changing the boundaries of the territory or state border of Ukraine, Article 110-2	0.5074	-0.1406	-0.8410
10	High treason, Article 111	0.5660	-0.1345	-0.7104
11	Collaboration activities, Article 111-1	0.7683	-0.3124	-0.4750
12	Aiding the aggressor state, Article 111-2	0.8398	-0.2755	-0.4137
13	Sabotage, Article 113	0.4972	-0.7640	-0.1682
14	Espionage, Article 114	0.4223	-0.3427	-0.8196
15	Obstruction of the lawful activities of the Armed Forces of Ukraine and other military formations, Article 114-1	0.6612	-0.6239	-0.1602
16	Illegal transportation of persons across the state border of Ukraine, Article 332	0.6361	0.0142	-0.6235
17	Various forms of evasion of military registration and conscription, Articles 335, 336 and 337	0.5831	-0.5551	-0.2848
18	Desecration of state symbols, Article 338	-0.0466	-0.8901	0.0075
19	Criminal offences against the established procedure for military service, Articles 402-435	0.6434	-0.6228	-0.1590
20	Justification, recognition as lawful or denial of the armed aggression of the russian federation against Ukraine, and glorification of its participants, Article 436-2	0.7683	-0.3124	-0.4750

Source: developed by the authors

The characteristics of factors F1, F2 and F3 are presented in Table 5. Table 5 suggests that the set of 20 features is, in effect, described by three latent dimensions, or factors, which have eigenvalues greater than one and together explain 86.52% of the total variance in the indicators under study.

Table 5. Characteristics of factors F1, F2 and F3

	Factor eigenvalue	Sum of squared factor loadings	Share of total variance explained by a particular factor	Cumulative explained variance
F1	13.8019	6.4046	0.3202	0.3202
F2	2.6136	4.5571	0.2279	0.5481
F3	1.3052	6.3415	0.3171	0.8652

Source: developed by the authors

The factor loading matrix presented confirms the research hypothesis concerning the existence of systemic relationships between the information influence of russian propaganda and criminal activity in the sphere of Ukraine's national security and defence capability. The first factor, F1, may be interpreted as a collaboration and destabilisation factor. The following features have the highest loadings on F1:

- No. 2 – "TCR";
- No. 11 – Article 111-1, collaboration activities;
- No. 12 – Article 111-2, aiding the aggressor state;
- No. 15 – Article 114-1, obstruction of the lawful activities of the Armed Forces of Ukraine;
- No. 16 – Article 332, illegal transportation of persons across the state border;
- No. 17 – evasion of military service, Articles 335-337[2];

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2341-14.
[2] Ibidem, 2001.

- No. 19 – offences against the procedure for military service, Articles 402-435;
- No. 20 – Article 436-2, justification of the russian federation's aggression.

This factor reflects a single complex of phenomena associated with the undermining of defence capability and evasion of mobilisation, the discrediting of military institutions, collaborationism and anti-state behaviour. It is particularly indicative that, among the propaganda terms, "TCR" has the highest loading on this factor, No. 2 = 0.884. This shows that campaigns aimed at discrediting the Armed Forces of Ukraine and, in particular, the TCR are statistically synchronised with collaboration activities, aiding the aggressor, offences against the procedure for military service and evasion of mobilisation. In criminological terms, this may point to the operation of a coordinated information influence aimed at weakening the state's mobilisation potential.

The second factor, F2, may be interpreted as a separatist and sabotage factor. The following features have the highest loadings on F2:

- No. 6 – "Novorossiya";
- No. 8 – Article 110, encroachment on territorial integrity;
- No. 13 – Article 113, sabotage;
- No. 15 – Article 114-1, obstruction of the activities of the Armed Forces of Ukraine;
- No. 18 – Article 338, desecration of state symbols;
- No. 19 – offences against the procedure for military service, Articles 402-435.

This factor primarily demonstrates a strong association between the term "Novorossiya" and Articles 110, 113 and 114-1[1]. In other words, it links separatist narratives with aggression against state symbols, acts of sabotage and encroachments on Ukraine's territorial integrity. This is consistent with the actual structure of russian hybrid aggression after 2014, in which the concept of "Novorossiya" was a central element in legitimising separatism, delegitimising Ukrainian statehood and stimulating sabotage activity. Thus, factor F2 can be regarded as a statistical manifestation of the separatist and sabotage-oriented strand of hybrid warfare.

The third factor, F3, may be interpreted as an ideological, repressive and occupation-related factor. The following features have the highest loadings on F3:

- No. 1 – "Bandera*";
- No. 3 – "Denazification";
- No. 4 – "Demilitarisation";
- No. 5 – "Capitulation";
- No. 7 – Article 109, violent change of the constitutional order;
- No. 9 – Article 110-2, financing actions against Ukraine;
- No. 14 – Article 114, espionage;
- No. 10 – Article 111, high treason;
- No. 16 – Article 332, illegal transportation of persons across the border.

This factor reflects the ideological justification of the russian federation's aggression, the propagandistic construction of the image of "Nazi Ukraine", narratives of coerced disarmament and capitulation, and the destruction of Ukrainian statehood. The most important terms here, as they have the highest loadings, are "Bandera*", "Denazification" and "Capitulation". These were key elements of russia's information support for the full-scale invasion of 2022. The factor association with the financing of anti-state activity, espionage and high treason indicates that this information cluster is statistically associated with more deep-seated forms of subversive activity. Overall, the identified latent factors of informational and criminogenic influence are shown in Table 6.

Table 6. Identified latent factors of informational and criminogenic influence

Factor	Probable content
F1	Collaborationism, mobilisation-related destabilisation and the undermining of defence capability
F2	Separatism, sabotage and anti-state symbolism
F3	Ideological justification of aggression and the undermining of statehood

Source: developed by the authors

The exploratory factor analysis showed the presence of common dynamics and synchronicity of changes between the number of propaganda materials related to specific russian information narratives and the statistics for particular types of registered criminal offences in Ukraine from 2013 onwards, as well as the existence of latent structures of interconnection. This supports the view that certain types of russian propaganda narratives are statistically interrelated with particular criminogenic processes in Ukraine.

Discussion

The method proposed in this study for identifying statistical links between media narratives and registered crimes is not entirely new in the international literature. Several research areas can serve as a methodological basis for the proposed approach and may be used in further studies on this topic. In particular, R. Marigliano *et al*. (2024) analyse large datasets from social media and apply cluster analysis, network analysis and statistical models to identify russian propaganda narratives and measure their intensity

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2341-14.

over time. Their study demonstrates that propaganda narratives can be represented as quantitative time series suitable for subsequent correlation or regression analysis. A. Biswas *et al*. (2023) use network analysis, clustering and narrative evolution analysis to construct time series of political messages. Although criminal statistics are not analysed in that study, the Article in effect proposes a method for transforming information campaigns into quantitative indicators.

M. Bozhidarova *et al*. (2023) propose using the correlation coefficient to assess the strength of statistical links between the spread of destructive narratives on social media and the dynamics of hate crimes. Although the study is not concerned with war, it provides a methodological basis for examining the influence of propaganda on criminal behaviour. C. Arcila Calderón *et al*.(2024)constructtimeseriesfortheintensityofmediacontent and official criminal statistics, calculate correlations, analyse lagged dependencies and build predictive models. This study convincingly demonstrates that media narratives may be statistically associated with registered crimes.

At the same time, there remains a gap in the literature concerning studies that directly establish a statistical relationship between the intensity of russian propaganda and officially registered criminal offences committed by citizens of Ukraine, such as collaboration activities, sabotage and high treason. Most of the studies considered analyse the relationship between propaganda, including disinformation, hate speech and incitement, and participation in violence, such as hate crimes, war crimes and genocide. In this study, the starting premise was that russian information narratives cause changes in social attitudes and emotional states among a certain proportion of Ukrainian citizens, contributing to their radicalisation, demoralisation and dehumanisation. This, in turn, provokes these citizens to commit unlawful acts that are reflected in statistically recorded categories of criminal offences. Such offences usually do not fall within the category of hate crimes, war crimes or genocide.

Conclusions

This study advanced a statistical hypothesis concerning the existence of consistency between changes in the number of registered offences under specific articles of the Criminal Code of Ukraine and changes in the number of russian-language anti-Ukrainian propaganda materials in russian media. It also advanced a research hypothesis concerning the existence of a certain latent structure linking indicators of the intensity of dissemination of particular russian propaganda narratives with indicators of the prevalence of specific types of criminal offences. Understanding the factor structure of the relationships between information and propaganda influence and criminogenic processes is a necessary precondition for developing strategies to counter the russian federation's information aggression and, accordingly, to reduce manifestations of certain types of criminal offences.

The rank correlation analysis identified statistically significant consistency between changes in the number of registered offences under specific articles of the Criminal Code of Ukraine and changes in the number of russian-language anti-Ukrainian propaganda materials on russian information and political television. It also produced quantitative indicators of the strength of the relationships between these dynamics (Table 3). The results of the rank correlation analysis confirmed the statistical hypothesis concerning the existence of relationships between changes in the number of registered offences under specific articles of the Criminal Code of Ukraine and changes in the number of russianlanguage anti-Ukrainian propaganda materials in russian media.

The study identified three distinct factors of informational and criminogenic influence. These factors combine the dynamics of russian propaganda narratives with the dynamics of indicators of criminal offences against the foundations of Ukraine's national security, statehood, defence capability and territorial integrity between 2013 and 2025. The factor structures obtained as a result of the analysis support the research hypothesis concerning the existence of a certain latent structure that determines the relationship between the intensity of russian propaganda information narratives transmitted to the civilian population of Ukraine and manifestations of criminal offences in the sphere of Ukraine's national security, statehood, defence capability and territorial integrity.

However, this study has limitations. In particular, the dynamics of the intensity with which particular russian propaganda narratives were used were assessed solely on the basis of russianlanguage content from russian information and political television, which provides only approximate indicators. Moreover, as the indicators of narrative intensity and criminal activity were presented on a yearly basis, this does not allow for taking into account time lags or guaranteeing the stability of the factor structure in factor analysis.

Further research is needed to extend the range of media outlets, as well as to take measurements of the russian propaganda intensity, on a monthly basis instead of yearly, to obtain more accurate estimates and to increase stability of the factor analysis. It would also be advisable to apply modern time series analysis methods, such as lag analysis, Granger causality and VAR models. In the cases where more detailed time-series data is available, these techniques may provide more informative results compared to correlation or factor analysis.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Alonso-Martín-Romo, L., Oliveros-Mediavilla, M., & Vaquerizo-Domínguez, E. (2023). Perception and opinion of the Ukrainian population regarding information manipulation: A field study on disinformation in the Ukrainian war. *El Profesional de la Información*, 32(4). doi: 10.3145/epi.2023.jul.05.

[2] Arcila Calderón, C., Sánchez Holgado, P., Gómez, J., Barbosa, M., Qi, H., Matilla, A., Amado, P., Guzmán, A., López-Matías, D., & Fernández-Villazala, T. (2024). From online hate speech to offline hate crime: The role of inflammatory language in forecasting violence against migrant and LGBT communities. *Humanities and Social Sciences Communications*, 11, article number 1369. doi: 10.1057/s41599-024-03899-1.

[3] Biswas, A., Niven, T., & Lin, Y.-R. (2023). The dynamics of political narratives during the Russian invasion of Ukraine. *arXiv*. doi: 10.1007/978-3-031-43129-6_4.

[4] Bozhidarova, M., Chang, J., Ale-Rasool, A., Liu, Y., Ma, C., Bertozzi, A.L., Brantingham, P.J., Lin, J., & Krishnagopal, S. (2023). Hate speech and hate crimes: A data-driven study of evolving discourse around marginalized groups. *arXiv*. doi: 10.48550/arXiv.2311.11163.

[5] Chaban, N., Zhabotynska, S., & Knodt, M. (2023). What makes strategic narrative efficient: Ukraine on Russian e-news platforms. *Cooperation and Conflict*, 58(4), 419-440. doi: 10.1177/00108367231161272.

[6] Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science*, 12(35). doi: 10.1140/epjds/s13688-023-00414-5.

[7] Goretzko, D., & Bühner, M. (2022). Robustness of factor solutions in exploratory factor analysis. *Behaviormetrika*, 49, 131-148. doi: 10.1007/s41237-021-00152-w.

[8] Hanley, H.W.A., & Durumeric, Z. (2024). Partial mobilization: Tracking multilingual information flows amongst russian media outlets and Telegram. *Proceedings of the International AAAI Conference on Web and Social Media*, 18(1), 528-541. doi: 10.1609/icwsm.v18i1.31332.

[9] Hladchenko, D. (2025). Analysis of the current criminal situation under articles 407 and 408 of the criminal code of Ukraine and the overview of the criminal law policy to counteract to these military criminal offences under martial law. *Current Problems of Domestic Jurisprudence*, 2, 110-118. doi: 10.32782/2408-9257-2025-2-18.

[10] Internews Network. (2024). *Ukrainian media, attitudes, and trust 2024*. Retrieved from https://surl.li/cnwfim.

[11] Katorkin, R. (2024). Determinants of collaboration activities. *Scientific Bulletin of the Dnipro State University of Internal Affairs*, 1, 44-51. doi: 10.31733/2078-3566-2024-1-44-51.

[12] Kopcha, V. (2025). Glorifier of russian aggression: Criminological characteristics of a person who commits a criminal offense under Article 436² of the Criminal Code of Ukraine. *Scientific Bulletin of Uzhhorod National University. Law Series*, 91(4), 95-99. doi: 10.24144/2307-3322.2025.91.4.11.

[13] Kudinov, V., Korneiko, O., & Pakrysh, O. (2025). Russia's information aggression against Ukraine: Dynamics and impact on the civilian population. *Juridical Scientific and Electronic Journal*, 8, 372-378. doi: 10.32782/2524-0374/2025-8/76.

[14] Kuksiuk, A. (2026). Criminological characteristics of an accomplice to an aggressor state. *Irpin Legal Chroniclles,* 4(21), 163-172. doi: 10.33244/2617-4154-4(21)-2025-163-172.

[15] Marigliano, R., Ng, L.H.X., & Carley, K.M. (2024). Analyzing digital propaganda and conflict rhetoric: A study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis. *Social Network Analysis and Mining*, 14, article number 170. doi: 10.1007/s13278-024-01322-w.

[16] Minenko, Y. (2023). The impact of Russian propaganda on the social and state stability of Ukraine: Analysis of methods and consequences. *Scientific works of Interregional Academy of Personnel Management Political Sciences and Public Management*, 3(69), 47-51. doi: 10.32689/2523-4625-2023-3(69)-6.

[17] Office of the Prosecutor General of Ukraine. (2026). *On registered criminal offenses and the results of their pre-trial investigation*. Retrieved from https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[18] Qiu, J., Li, Z., & Yao, J. (2025). Robust estimation for number of factors in high dimensional factor modeling via Spearman Correlation Matrix. *Journal of the American Statistical Association*, 120(550), 1139-1151. doi: 10.1080/01621459.2024.2402565.

[19] Rawnak. (2025). The role of hate speech in inciting genocide: A case study of Radio Television Libre des Mille Collines in Rwanda. *Contemporary Challenges: The Global Crime, Justice and Security Journal*, 5. doi: 10.2218/ccj.v5.10257.

[20] Rudnieva, A., & Malovana, Y. (2026). The russian federation's information war against Ukraine in 2025: Analysis of key narratives and psychological mechanisms of influence. *Newsletter of Precarpathian University. Politology*, 22, 18-25. doi: 10.32782/2312-1815/2025-22-35.

[21] Sidchenko, S., Zalkin, S., Khudarkovskyi, K., & Bielimov, V. (2024). Informational (psychological) impact of Russian propaganda on young people in the russian federation and on the temporarily occupied territories of Ukraine. *Collection of Scientific Papers of the Kharkiv National Air Force University*, 1(79), 113-118. doi: 10.30748/zhups.2024.79.17.

[22] Sviderska, O. (2022). Digital propaganda and risks of information security in the context of the Russian-Ukrainian war. *Politicus: Scientific Journal*, 2, 60-65. doi: 10.24195/2414-9616.2022-2.10.

[23] Tatarenko, H. (2026). History of the formation and transformation of the specialized prosecutor's office in the field of defence of Ukraine (1991-2025): Problems and prospects. *Topical Issues of Law: Theory and Practice*, 1(51), 236-248. doi: 10.33216/2218-5461/2026-51-1-236-248.
[24] War of Words. (2026). *The service for analyzing Russian information-political TV and RuTube*. Retrieved from https://warofwords.info/.
[25] Zalkin, S., Sidchenko, S., Khudarkovskyi, K., Revin, O., Bielimov, V., & Svystunov, D. (2025). Systematic analysis of narratives of the russian federation's information war against Ukraine according to NATO standards. *Collection of scientific papers of the Kharkiv National Air Force University*, 3(85), 93-102. doi: 10.30748/zhups.2025.85.12.

Взаємозв'язок російської пропаганди та певних криміногенних процесів в Україні

Вадим Кудінов
Кандидат фізико-математичних наук, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-5299-0590
Олександр Пакриш
Кандидат технічних наук, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-6420-5246
Юлія Панімаш
Кандидат педагогічних наук
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту
18034, вул. Онопрієнка, 8, м. Черкаси, Україна
https://orcid.org/0000-0002-5337-6613

Анотація
У статті досліджено вплив російських інформаційно-психологічних операцій на суспільну свідомість українців з метою провокування кримінальних правопорушень. Інтенсивність російських наративів оцінено шляхом контент-аналізу частоти появи окремих російськомовних термінів у пропагандистських матеріалах. Кількість окремих видів кримінальних правопорушень визначено на основі статистичної звітності Офісу Генерального прокурора. Дослідження виявило статистично значущу узгодженість динаміки змін кількості пропагандистських матеріалів з окремих російських інформаційно-психологічних операцій та динаміки змін окремих видів зареєстрованих злочинів в Україні за період з 2013 до 2025 року. На основі здійсненого кореляційного аналізу сформовано припущення щодо впливу певних пропагандистських наративів на статистичні дані з окремих видів кримінальних правопорушень. За результатами факторного аналізу виявлено наявність трьох окремих чинників інформаційно-криміногенного впливу, які об'єднують динаміку російських пропагандистських наративів і показників кримінальних правопорушень проти основ національної безпеки, державності, обороноздатності й територіальної цілісності України за період з 2013 до 2025 року. Встановлення наявності впливу російської пропаганди на статистику кримінальних правопорушень і факторів, що зумовлюють цей вплив, дасть змогу визначати стратегії щодо зниження ефективності російської пропаганди та рівня злочинності

Ключові слова:
інформаційно-психологічні операції; інформаційні наративи; кримінальні правопорушення; рівень злочинності; рангова кореляція; факторний аналіз

UDC 347.734: 346.7
DOI: 10.63341/naia-chasopis/2.2026.42

ISSN 2519-4216
E-ISSN 2519-4313

Legal regulation of the banking system in Ukraine in the context of European integration: A comparative legal analysis with EU legislation

Andriy Tsvyetkov*
PhD in Law, Senior Researcher
F.G. Burchak Research Institute of Private Law and Entrepreneurship
of the National Academy of Legal Sciences of Ukraine
03150, 11 Kazimir Malevich Str., Kyiv, Ukraine
https://orcid.org/0000-0002-3239-322X

Abstract
The study aimed to compare the legal regulation of Ukraine's banking system with European legal standards to identify areas for its further improvement. Methods of doctrinal-legal, comparative-legal and systemic-structural analysis were employed. The results of the study showed that the harmonisation of Ukraine's banking legislation with EU law is uneven. The most pronounced substantive similarity between the models is evident in the prudential block and related areas of risk management, supervisory reporting and financial monitoring, whilst the most notable differences concern anti-crisis regulation, the organisation of supervision and the integration of digital operational resilience and cyber risks into banking supervision. In both models, legal regulation was aimed at ensuring the stability of the banking system, risk control, depositor protection and the consideration of related non-financial risks, particularly in the areas of financial monitoring, data protection and cybersecurity. It has been established that the Ukrainian model of approximation to EU law is predominantly functional in nature, as it replicates the substance and methods of European banking regulation but cannot fully replicate the supranational institutional architecture of the European Banking Union. In this regard, the further alignment of Ukraine's banking legislation with EU law involves not only updating specific provisions, but also strengthening systemic coherence between the prudential, supervisory, crisis management and digital regulatory frameworks. Therefore, the further adaptation of Ukrainian legislation to EU law requires the standardisation of supervisory reporting, the development of mechanisms for resolving banking crises, and the integration of digital operational resilience. The practical significance of the results is determined by their potential use by the National Bank of Ukraine, government bodies and academic and educational institutions to improve banking legislation, adapt it to European law and incorporate it into the educational process

Keywords:
legal risk management; regulation of financial monitoring; harmonisation of legislation; legal partnership between the state and business; legal liability; legal regulation of market relations

Article's History:
Received: 06.01.2026
Revised: 06.04.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Tsvyetkov, A. (2026). Legal regulation of the banking system in Ukraine in the context of European integration: A comparative legal analysis with EU legislation. *Law Journal of the National Academy of Internal Affairs*, 16(2), 42-61. doi: 10.63341/naia-chasopis/2.2026.42.

*Corresponding author (*Andriy_Tsvyetkov@outlook.com*)

Introduction

In the context of Ukraine's European integration process, the banking system is one of the areas in which regulatory alignment with EU law is systematic. The legal regulation of banking activities covers issues relating to financial market stability, the functioning of credit institutions and the protection of consumers of financial services. Under martial law, the quality of such regulation affects the continuity of the banking sector's operations and the country's overall economic stability. At the same time, the harmonisation of Ukraine's banking legislation with EU law is proceeding unevenly, which necessitates a review of existing changes and the identification of those elements of legal regulation that remain fragmented or incomplete.

The works of European researchers have established a theoretical foundation for a comparative legal analysis of banking legislation in Ukraine and the EU. G. Lo Schiavo (2024) noted that EU banking law has developed as a supranational regulatory system encompassing institutional supervisory mechanisms, bank insolvency resolution and uniform rules for credit institutions. The development of banking regulation in Europe, as shown in the study by K. Parchimowicz (2023), was a transition from a reactive response to financial crises to proactive legal regulation of risks. The formation of the European Banking Union and the introduction of centralised supervisory and regulatory mechanisms aimed at enhancing the resilience of the banking system was central in this process. The author emphasised that the harmonisation of prudential requirements and enhanced coordination between national and supranational institutions facilitated the transition to a systemic and risk-based approach in banking regulation.

As W.P. de Groen (2023) has noted, the European Banking Union has strengthened its supervisory and crisis management mechanisms, although legal, economic, political and operational challenges remain in this area. In particular, the author highlighted the incompleteness of the European Banking Union's institutional architecture, notably in a common deposit guarantee scheme, which limits the achievement of full financial market integration. D. Vese (2025) argued that the discretionary powers of the European Banking Authority must be exercised through the prism of the public interest and the proper protection of individual and collective rights. The author emphasised that the expansion of the discretion of supranational regulators requires clear legal boundaries and accountability mechanisms, particularly in supervisory decisions and regulatory intervention.

According to O. Hülsewig & A. Steinbach (2025), the interaction between prudential banking regulation and fiscal rules can cause systemic imbalances, as preferential regulatory treatment of government bonds undermines fiscal discipline and strengthens the link between banks and sovereign debt. The authors argue that such a framework creates additional macro-financial risks and may reduce the effectiveness of prudential supervision, as it encourages the concentration of risks on bank balance sheets. Studies on the procedural aspects of the exercise of supervisory powers are substantial for interpretation of the contemporary model of banking supervision in the 21st-century EU. In particular, M. Lamandini *et al.* (2022) examined the Supervisory Review and Evaluation Process as a key mechanism for the practical exercise of supervisory powers in European banking law. A separate area concerns the expansion of the scope of financial regulation to include digital risks. D. Clausmeier (2023) demonstrated that digital operational resilience in EU law has acquired the status of an independent area of regulation linked to ensuring the stability of the financial sector. The author found that information and communication technology risks, cyber threats and dependence on external digital suppliers are no longer viewed as purely technical issues, but are integrated into the supervisory assessment framework for financial institutions.

The Ukrainian debate has focused on the implementation of the EU's financial acquis and the transformation of the national banking regulatory model in the context of European integration. The study by E. Dmytrenko (2021) noted that the implementation of EU standards in the field of banking relations must be conducted following Ukraine's obligations under the Association Agreement and entails updating not only individual regulatory provisions but also the principles of banking regulation and supervision. P.S. Patsurkivskyi & R.O. Havryliuk (2025) emphasised that Ukraine's implementation of the EU financial acquis is gradually becoming more comprehensive and covers key segments of financial regulation, in particular the banking sector.

Thus, a review of the literature has shown that existing studies examine the architecture of EU banking law, the evolution of supervisory and crisis management mechanisms, procedural aspects of banking supervision, as well as specific areas of alignment between Ukrainian legislation and EU law. At the same time, there is no systematic comparison in which the banking legislation of Ukraine and the EU would be systematically compared not only at the level of individual provisions, but also within the framework of a comprehensive system of prudential regulation, crisis resolution, supervisory reporting, deposit guarantees, digital resilience and the institutional organisation of banking supervision. Therefore, the study aimed to identify the common and distinctive features of the legal regulation of Ukraine's banking system in relation to European legal standards to determine areas for its further improvement. To achieve this aim, the following tasks were set: to ascertain the content and structure of the regulatory framework for the EU banking

system; to analyse the legal foundations of the functioning of the Ukrainian banking system and the extent to which it aligns with European legal standards; and to identify existing gaps in Ukrainian banking legislation compared to EU law to determine prospects for further improvement.

Materials and Methods

This study is qualitative in nature and was based on the application of doctrinal-legal, comparative-legal and systemic-structural methods to analyse the legal foundations for the regulation and harmonisation of Ukrainian banking legislation with EU law. Doctrinal-legal analysis was used to examine EU legal acts and Ukrainian legislative acts in the field of banking regulation. Within the framework of this method, an interpretation was conducted of the key legal categories, principles and approaches that define prudential regulation (in particular, requirements for capital, liquidity and risk management), the model of banking supervision, and the legal mechanisms for crisis resolution and deposit guarantees. The analysis of related regulation affecting banking activities, particularly in the areas of financial monitoring, personal data protection, digital operational resilience and cybersecurity, was emphasised. This determined the scope and rationale behind the development of banking regulation in both EU law and Ukrainian legislation, and established a conceptual framework for further comparative legal analysis.

A comparative legal analysis was used to compare EU law and Ukrainian legislation according to the following criteria: the subject matter of legal regulation, the institutional model of banking supervision, capital and risk management requirements, supervisory reporting, mechanisms for resolving bank insolvency, depositor protection, as well as regulation in the areas of financial monitoring, digital operational resilience and cybersecurity, which made it possible to identify similarities, differences and gaps. The study utilised EU and Ukrainian regulatory acts governing banking activities. The regulatory framework is structured into functional blocks: prudential and supervisory regulation; crisis management mechanisms covering recovery, bank insolvency resolution and deposit guarantees; as well as related regulation in the areas of financial monitoring, personal data protection, digital operational resilience and cybersecurity. Separately, international legal and institutional sources have been used, which form the basis for the harmonisation of Ukraine's banking legislation with EU law (Table 1).

Table 1. A comprehensive database of EU and Ukrainian legislation

Functional unit	EU acts	Laws of Ukraine	Aspects of legal regulation under consideration
Prudential and supervisory regulation	Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions"; Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms", Regulation European Parliament and the Council of the European Union No. 575/2013; European Commission Implementing Regulation No. 2024/3117; Directive of the European Parliament and the Council of the European Union No. 2024/1619; Regulation of the European Parliament and the Council of the European Union No. 2024/1623	Law of Ukraine No. 2121-III "On Banks and Banking", Law of Ukraine No. 679-XIV "On the National Bank of Ukraine", Resolution of the National Bank of Ukraine No. 196, Resolution of the National Bank of Ukraine No. 64, Resolution of the National Bank of Ukraine No. 161, Resolution of the National Bank of Ukraine No. 120, Decision of the National Bank of Ukraine No. 814-rsh, Resolution of the Board of the National Bank of Ukraine No. 23 "On Some Issues of Operation of Ukrainian Banks and Banking Groups"	Banking authorisation, capital requirements, liquidity, risk management, corporate governance, supervisory powers, supervisory reporting
Crisis management mechanisms	Regulation of the European Parliament and the Council of the European Union No. 806/2014; Directive of the European Parliament and the Council of the European Union No. 2014/59/EU; Directive of the European Parliament and the Council of the European Union No. 2014/49/EU	Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits"	Bank recovery and resolution, deposit guarantees, and mechanisms for responding to banking crises
Related regulations	Regulation of the European Parliament and the Council of the European Union No. 2016/679; Regulation European Parliament and the Council of the European Union No. 2022/2554; Directive of the European Parliament and the Council of the European Union No. 2022/2555, Regulation of the European Parliament and the Council of the European Union No. 2024/1620; Regulation of the European Parliament and the Council of the European Union No. 2024/1624; Directive of the European Parliament and the Council of the European Union No. 2024/1640	Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction", Law of Ukraine No. 2297-VI "On Protection of Personal Data", Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine"	Financial monitoring, data protection, digital operational resilience, cybersecurity

Table 1, Continued

Functional unit	EU acts	Laws of Ukraine	Aspects of legal regulation under consideration
The international legal and institutional framework for harmonisation	Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part	The NBU's assessment of the alignment of national legislation on financial services with EU law as part of the screening process	The legal and institutional framework for harmonising Ukrainian banking legislation with EU law

Source: compiled by the author based on Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions"[1], Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC"[2], Directive of the European Parliament and the Council of the European Union No. 2014/59/EU "Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms and Amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No. 1093/2010 and (EU) No. 648/2012"[3], Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No. 648/2012 (Capital Requirements Regulation, CRR)"[4], Regulation of the European Parliament and the Council of the European Union No. 806/2014 "Establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No. 1093/2010"[5], Regulation of the European Parliament and the Council of the European Union No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing"[6], Directive of the European Parliament and the Council of the European Union No. 2024/1640 "On the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, amending Directive (EU) 2019/1937, and amending and Repealing Directive (EU) 2015/849"[7], Directive of the European Parliament and the Council of the European Union No. 2014/49/EU "On Deposit Guarantee Schemes (Recast)"[8], Regulation of the European Parliament and the Council of the European Union No. 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)"[9], Law of Ukraine No. 2121-III "On Banks and Banking"[10], Law of Ukraine No. 679-XIV "On the National Bank of Ukraine"[11], Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits"[12], Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons

[1] Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions". (2013, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/1024/oj/eng.
[2] Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/dir/2013/36/oj/eng.
[3] Directive of the European Parliament and the Council of the European Union No. 2014/59/EU "Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms". (2014, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/59/oj/eng.
[4] Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No. 648/2012 (Capital Requirements Regulation, CRR)". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/575/oj/eng.
[5] Regulation of the European Parliament and the Council of the European Union No. 806/2014 "Establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No. 1093/2010". (2014, July). Retrieved from https://eur-lex.europa.eu/eli/reg/2014/806/oj/eng.
[6] Regulation of the European Parliament and the Council of the European Union No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng.
[7] Directive of the European Parliament and the Council of the European Union No. 2024/1640 "On the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing,". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng.
[8] Directive of the European Parliament and the Council of the European Union No. 2014/49/EU "On Deposit Guarantee Schemes (Recast)". (2014, April). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/49/2014-07-02/eng.
[9] Regulation of the European Parliament and the Council of the European Union No. 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)". (2016, April). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/eng.
[10] Law of Ukraine No. 2121-III "On Banks and Banking". (2000, December). Retrieved from https://zakon.rada.gov.ua/go/2121-14?lang=en.
[11] Law of Ukraine No. 679-XIV "On the National Bank of Ukraine". (1999, May). Retrieved from https://bank.gov.ua/en/legislation/Law_NBU.
[12] Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits". (2012, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4452-17?lang=en.

of Mass Destruction"[1], Law of Ukraine No. 2297-VI "On Protection of Personal Data"[2], Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine"[3], Resolution of the Board of the National Bank of Ukraine No. 23 "On Some Issues of Operation of Ukrainian Banks and Banking Groups"[4], Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part[5], Resolution of the National Bank of Ukraine No. 196 "On Approval of the Regulation on the Procedure for Determining the Regulatory Capital by Ukrainian Banks"[6], Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups"[7], Resolution of the National Bank of Ukraine No. 161 "On Approval of the Regulation on Organization of Internal Capital Adequacy Assessment Process (ICAAP) in Banks of Ukraine and Banking Groups"[8], Resolution of the National Bank of Ukraine No. 120 "On Approval of the Rules of Management of Statistical Reporting Filed with the NBU"[9]

The selection of these regulatory acts is based on the fact that they represent the key levels and components of the European and Ukrainian models of banking regulation and can be used for an analysis of the prudential, institutional, anti-crisis and related regulatory frameworks, as well as to trace how, in Ukrainian law, the institutional foundations of the banking system are combined with practical supervisory mechanisms and its functional alignment with EU law. The choice of a timeframe starting from 2013 is determined by the fact that during this period, the regulatory framework for the banking system was established in EU law, and the subsequent changes from 2014 to 2024 reflect its institutional and functional development. This was done to identify the structural elements of EU and Ukrainian banking law and to establish a regulatory framework for the subsequent analysis of the harmonisation of Ukrainian banking legislation with EU law.

The systemic-structural approach has been applied to examine banking regulation as a coherent legal system comprising interrelated regulatory, institutional and functional elements. Within this framework, the legal regulation has been organised into key components: prudential regulation, banking supervision, crisis management mechanisms and ancillary regulation. This made it possible to analyse the interrelationships between these blocks, their role in ensuring the stability of the banking system, and to identify areas where the greatest substantive similarities or differences between the legal regulation of Ukraine and the EU can be observed. The comparison of the legal regulation of banking activities in the EU and Ukraine was conducted based on differences in the levels of legal regulation, in particular the supranational nature of EU law and the national nature of Ukrainian banking legislation, which was used as one of the criteria for comparative legal analysis. Within this approach, the legal regulation was structured according to key functional blocks. This established systemic links between individual elements of banking regulation, identified the degree of their coherence, and determined the segments in which the harmonisation of Ukrainian legislation with EU law is of a most comprehensive or, conversely, fragmentary nature. A limitation of the study was the theoretical and legal nature, which resulted in the absence of an analysis of legal practice and empirical data, and prevented a quantitative assessment of the effectiveness of the mechanisms for harmonising Ukrainian banking legislation with EU law.

Results and Discussion

The legal framework for the regulation of the banking systems in the EU and Ukraine

The legal framework governing the EU banking system is a comprehensive, multi-tiered system in which prudential requirements, supranational supervision, bank crisis resolution and related control regimes operate in tandem. EU banking law is aimed not only at

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20?lang=en.
[2] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en.
[3] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.
[4] Resolution of the Board of the National Bank of Ukraine No. 23 "On Some Issues of Operation of Ukrainian Banks and Banking Groups". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/v0023500-22.
[5] Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. (2014, June). Retrieved from https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj/eng.
[6] Resolution of the National Bank of Ukraine No. 196 "On Approval of the Regulation on the Procedure for Determining the Regulatory Capital by Ukrainian Banks". (2023, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_28122023_196.
[7] Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups". (2018, June). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_11062018_64.
[8] Resolution of the National Bank of Ukraine No. 161 "On Approval of the Regulation on Organization of Internal Capital Adequacy Assessment Process (ICAAP) in Banks of Ukraine and Banking Groups". (2021, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_30122021_161.
[9] Resolution of the National Bank of Ukraine No. 120 "On Approval of the Rules of Management of Statistical Reporting Filed with the NBU". (2018, November). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_13112018_120.

authorisation to operate or capital requirements, but also at preventing systemic risk; therefore, a bank is regarded as an institution of public importance for the Union's internal market. A key feature of EU banking law is the transition from minimal coordination of national regimes to a single regulatory framework in the field of banking supervision. It is based on a combination of Directive 2013/36/EU of the European Parliament and of the Council[1] and Regulation (EU) No. 575/2013 of the European Parliament and of the Council[2]: the former stipulated the institutional framework for access to banking activities, requirements for internal governance, control and supervisory powers, whilst the latter establishes uniform requirements for capital, liquidity, large exposures, leverage and disclosure. This approach demonstrates that, under EU law, a bank is regarded not as an ordinary business entity, but as an institution whose stability is of public importance. Therefore, financial stability is linked not only to capital adequacy but also to the quality of internal governance, the transparency of the ownership structure, the sound business reputation of managers, and the ability to operate under constant supervision.

Further amendments in 2024 confirmed the development of this model. Directive 2024/1619 of the European Parliament and of the Council of the European Union[3] broadened the scope of supervisory control by including the powers of supervisory authorities, the regime for third-country branches and the consideration of environmental, social and governance risks. Regulation of the European Parliament and the Council of the European Union No. 2024/1623[4] updated the approaches to assessing credit, market and operational risk, strengthening the requirements for capital coverage of risks. A key element of this system is also supervisory reporting, the standardisation of which ensures the uniform application of prudential rules across the EU in accordance with European Commission Implementing Regulation No. 2024/3117[5]. Thus, in the field of prudential regulation, the EU has developed a comprehensive model in which authorisation to conduct banking activities, capital requirements, risk management, reporting and supervision form a single system designed to ensure stability.

If the Directive of the European Parliament and the Council of the European Union No. 2013/36/EU[6] stipulate the substantive core of banking supervision, then Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions"[7] shapes its institutional architecture. The significance of this act is determined by the reflection of the EU's conclusion following the financial crisis: an integrated banking market cannot be stable if national supervision remains completely fragmented. The introduction of the Single Supervisory Mechanism within the European Banking Union meant a partial transfer of supervisory powers to the supranational level. The transfer of key functions to the European Central Bank demonstrated that the national model of supervision is insufficient for banks whose activities are cross-border in nature. This approach aims not only to standardise supervisory standards, but also to reduce the risk of national authorities being lenient towards domestic large banks. At the same time, this system does not imply complete centralisation. National competent authorities are not removed from supervision, but operate within a common multi-level model, where the European Central Bank fulfils a strategic role, whilst national authorities retain a significant proportion of practical functions. Therefore, the EU's institutional model combines supranational coordination with the participation of national regulators.

In the context of banking crises, EU law is based on the premise that a bank's insolvency has not only private-law implications but also systemic consequences, and is therefore subject to specific public-law regulation. Such model was stipulated in the Directive of the

[1] Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/dir/2013/36/oj/eng.

[2] Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms (Capital Requirements Regulation, CRR)". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/575/oj/eng.

[3] Directive of the European Parliament and the Council of the European Union No. 2024/1619 "Amending Directive 2013/36/EU as Regards Supervisory Powers, Sanctions, Third-Country Branches, and Environmental, Social and Governance Risks". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2024/1619/oj/eng.

[4] Regulation of the European Parliament and the Council of the European Union No. 2024/1623 "Amending Regulation (EU) No. 575/2013 as Regards Requirements for Credit Risk, Credit Valuation Adjustment Risk, Operational Risk, Market Risk and the Output Floor". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1623/oj/eng.

[5] European Commission Implementing Regulation No. 2024/3117 "Laying Down Implementing Technical Standards for the Application of Regulation (EU) No. 575/2013 of the European Parliament and of the Council with Regard to Supervisory Reporting of Institutions and Repealing Commission Implementing Regulation (EU) 2021/451". (2024, November). Retrieved from https://eur-lex.europa.eu/eli/reg_impl/2024/3117/oj/eng.

[6] Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms (Capital Requirements Regulation, CRR)". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/575/oj/eng.

[7] Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions". (2013, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/1024/oj/eng.

European Parliament and the Council of the European Union No. 2014/59/EU[1], which established the legal framework for the recovery and resolution of banks. It involves a shift from an approach whereby a bank is either bailed at public expense or wound up under standard rules, to a regime of managed intervention in the interests of financial stability. One of the central elements of this model is that losses are covered primarily by the bank's shareholders and creditors. This approach enshrines another principle of banking risk allocation: losses in the private financial sector should not automatically be passed on to the state if the legal system provides mechanisms for their internal absorption.

Regulation of the European Parliament and the Council of the European Union No. 806/2014[2] builds on this model by shifting crisis management within the European Banking Union from the national to the supranational level. Its function is to ensure a coordinated response to banking crises within the single market when preventive mechanisms are no longer sufficient. Directive of the European Parliament and of the Council of the European Union No. 2014/49/EU[3] defines another element of this framework. Its purpose is not only to protect depositors but also to maintain confidence in the banking system, without which even a financially sound sector may be vulnerable to panic and a liquidity crisis. Together, these acts form an anti-crisis model that combines prevention, managed intervention, loss sharing and depositor protection.

Modern 21st-century EU banking law covers not only traditional financial issues but also related areas that were previously considered separately from banking supervision. This means that a bank's resilience is assessed not only in terms of capital and liquidity, but also in terms of its ability to ensure data protection, digital operational resilience, cybersecurity and compliance with anti-money laundering requirements. Regulation (EU) 2016/679 of the European Parliament and of the Council[4] establishes legal requirements for the banking sector regarding the processing of personal data, and breaches of these requirements affect the assessment of an institution's reliability. Regulation (EU) No. 2022/2554 of the European Parliament and of the Council[5], establishes digital operational resilience as a component of the supervisory regime, as failures in information and communication infrastructure, cyber-attacks or dependence on external technology service providers may have systemic consequences. Directive 2022/2555 of the European Parliament and of the Council of the European Union[6], in turn, treats cybersecurity as an element of critical infrastructure protection, which also extends to the banking sector. The 2024 EU acts in the field of preventing money laundering and terrorist financing, in particular Regulation of the European Parliament and of the Council No. 2024/1620[7], Regulation of the European Parliament and of the Council of the European Union No. 2024/1624[8], Directive of the European Parliament and of the Council of the European Union No. 2024/1640[9] indicate a further centralisation of this area, the harmonisation of substantive requirements and the refinement of control mechanisms for Member States (Fig. 1).

Under EU law, a bank is assessed not only based on its financial performance, but also on its ability to ensure data protection, digital and cyber resilience, and compliance with financial monitoring requirements. This provides grounds for viewing EU banking law as a comprehensive regulatory resilience framework that combines prudential requirements, the institutional organisation of supervision, mechanisms for resolving banking crises, and related legal control regimes. The European model is not a collection of isolated regulatory acts, but an interconnected framework for ensuring the stability of the banking sector.

[1] Directive of the European Parliament and the Council of the European Union No. 2014/59/EU "Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms". (2014, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/59/oj/eng.
[2] Regulation of the European Parliament and the Council of the European Union No. 806/2014 "Establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund". (2014, July). Retrieved from https://eur-lex.europa.eu/eli/reg/2014/806/oj/eng.
[3] Directive of the European Parliament and the Council of the European Union No. 2014/49/EU "On Deposit Guarantee Schemes (Recast)". (2014, April). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/49/2014-07-02/eng.
[4] Regulation of the European Parliament and the Council of the European Union No. 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)". (2016, April). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/eng.
[5] Regulation European Parliament and the Council of the European Union No. 2022/2554 "On Digital Operational Resilience for the Financial Sector". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.
[6] Directive of the European Parliament and the Council of the European Union No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive)". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.
[7] Regulation of the European Parliament and the Council of the European Union No. 2024/1620 "Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng.
[8] Regulation of the European Parliament and the Council of the European Union No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng.
[9] Directive of the European Parliament and the Council of the European Union No. 2024/1640 "On the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng.

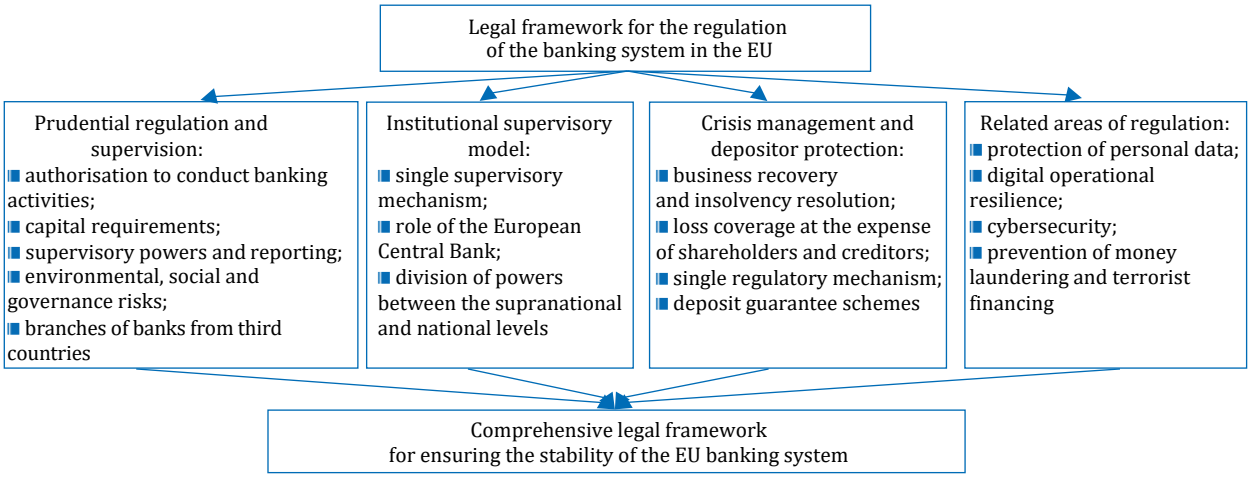

Figure 1. Framework for the regulatory and legal supervision of the EU banking system
Source: compiled by the author

In contrast to EU law, which operates within a supranational legal framework and a multi-tiered system of banking supervision, the Ukrainian model of banking regulation is national in nature and is based on a combination of framework laws and regulatory acts issued by the National Bank of Ukraine. The laws define the institutional foundations of the banking system and the basic rules governing the market, whilst the NBU specifies the prudential, supervisory and organisational requirements for banks. At the same time, Ukrainian banking legislation covers not only the legal framework for banking activities, but also depositor protection, mechanisms for removing insolvent banks from the market, as well as related areas such as anti-money laundering, personal data protection and cybersecurity. It can therefore be regarded as a comprehensive national system for ensuring the stability of the banking sector. Law of Ukraine No. 679-XIV[1] enshrines the public-law nature of banking supervision, defining the NBU not only as the central bank but also as the body responsible for regulatory coordination, through which the monetary function, the maintenance of financial stability and banking supervision are combined.

Law of Ukraine No. Law No. 2121-III[2] establishes the basic institutional framework for banking law, distinguishing banking activities from general economic activities and subjecting them to a special regime governing establishment, licensing, supervision and liability. Within this model, a bank is regarded as a special entity subject to heightened requirements regarding transparency, capital, ownership structure and internal governance. This indicates that the Ukrainian model of banking regulation combines the institutional level of legislative definition of a bank's status with the functional level of detail regarding supervisory and prudential requirements in the NBU's regulatory acts.

Law of Ukraine No. Law No. 4452-VI[3] establishes a separate mechanism for protecting depositors and maintaining confidence in the banking system. Within the framework of the Ukrainian model, this law defines the legal basis for the operation of a special fund through which guarantees for depositors and procedures for removing insolvent banks from the market are implemented. Thus, depositor protection and the response to bank insolvency in Ukraine are institutionally linked to the activities of a separate national mechanism that performs not only a compensatory but also a stabilising function. Law of Ukraine No. 361-IX[4] establishes a risk-based approach in the field of anti-money laundering, under which banks are required to establish internal mechanisms for the identification, assessment and control of high-risk transactions. This indicates the integration of financial monitoring into a broader system of internal control and risk management in banking activities. Law of Ukraine No. 2297-VI[5] and Law of Ukraine No. 2163-VIII[6] demonstrate that banking regulation in

[1] Law of Ukraine No. 679-XIV "On the National Bank of Ukraine". (1999, May). Retrieved from https://bank.gov.ua/en/legislation/Law_NBU.
[2] Law of Ukraine No. 2121-III "On Banks and Banking". (2000, December). Retrieved from https://zakon.rada.gov.ua/go/2121-14?lang=en.
[3] Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits". (2012, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4452-17?lang=en.
[4] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20?lang=en.
[5] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en.
[6] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.

Ukraine also covers the related areas of personal data protection and cybersecurity. Consequently, the stability of banking operations within the national legal framework is linked not only to financial indicators but also to a banking institution's ability to ensure the protection of personal data and to counter cyber risks. In structural terms, this means that the Ukrainian model of banking regulation already goes beyond narrow prudential supervision and encompasses a broader range of legal instruments to ensure the stability of the banking sector.

Whilst legislation stipulates the general framework for banking regulation, the National Bank of Ukraine's regulations provide the level of detail required to specify the prudential, supervisory and organisational requirements for banks. The main provisions regarding capital, risk management, reporting and corporate governance are concentrated in subordinate legislation. Resolution of the National Bank of Ukraine No. 196[1] details the legislative requirements for capital as a tool for covering banking risks. Resolution of the National Bank of Ukraine No. 64[2] establishes requirements for internal procedures for the identification, measurement, control and monitoring of risks. This regulatory logic is further developed in Resolution of the National Bank of Ukraine No. 161[3], which obliges banks to conduct an internal assessment of capital adequacy based on risk profile and to justify it to the supervisory authority.

The NBU's regulations on reporting and corporate governance also demonstrate that banking supervision in Ukraine is not limited to a formal check of compliance with specific standards. Resolution of the National Bank of Ukraine No. 120[4], and Decision of the National Bank of Ukraine No. 814-rsh[5] indicate that reporting and a bank's internal organisation are regarded as components of the supervisory regime, upon which the transparency of the bank's activities, the quality of risk-taking and the effectiveness of internal control depend. Of particular significance is Resolution of the Board of the National Bank of Ukraine No. 23[6], which reflects the specific nature of the Ukrainian legal context, within which prudential regulation is combined with the need to ensure the continuity of the banking system's functioning under martial law. This provides grounds for asserting that the Ukrainian model of banking regulation has a two-tier structure: the legislative level defines the institutional foundations and general rules, whilst the sub-legislative level, established by NBU acts, ensures the functional specification of prudential supervision. This structure highlights the key role of the NBU not only as a banking supervisory authority, but also as an entity whose regulatory framework effectively shapes the practical architecture of Ukraine's banking system (Fig. 2).

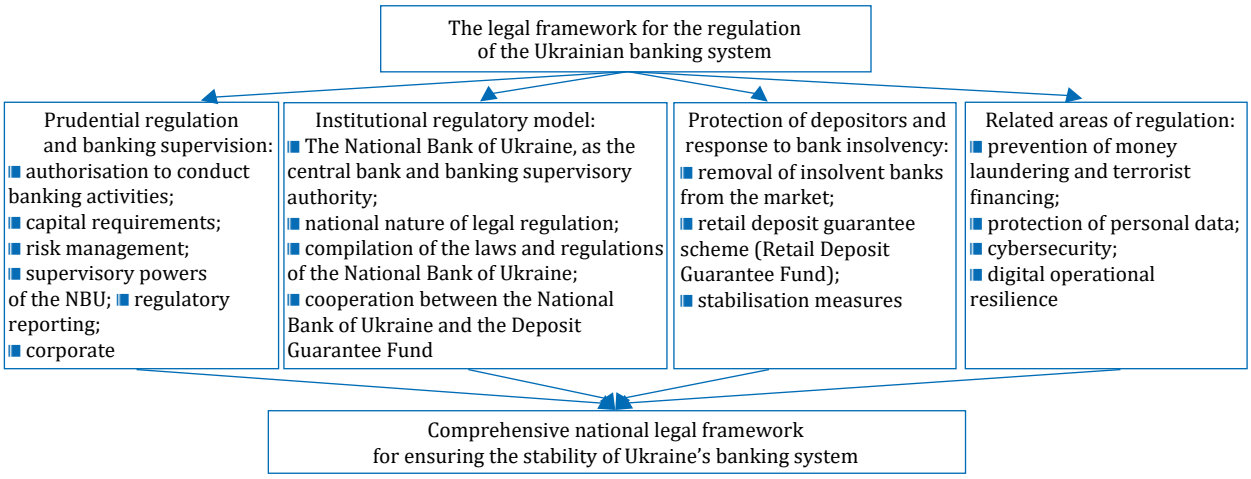

Figure 2. Structure of the national regulatory framework for the banking system in Ukraine and areas of alignment with EU law

Source: compiled by the author

[1] Resolution of the National Bank of Ukraine No. 196 "On Approval of the Regulation on the Procedure for Determining the Regulatory Capital by Ukrainian Banks". (2023, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_28122023_196.

[2] Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups". (2018, June). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_11062018_64.

[3] Resolution of the National Bank of Ukraine No. 161 "On Approval of the Regulation on Organization of Internal Capital Adequacy Assessment Process (ICAAP) in Banks of Ukraine and Banking Groups". (2021, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_30122021_161.

[4] Resolution of the National Bank of Ukraine No. 120 "On Approval of the Rules of Management of Statistical Reporting Filed with the NBU". (2018, November). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_13112018_120.

[5] Decision of the National Bank of Ukraine No. 814-rsh "On Approval of the Methodological Recommendations on Organization of Corporate Governance in Banks of Ukraine". (2018, December). Retrieved from https://bank.gov.ua/ua/legislation/Decision_03122018_814-rsh.

[6] Resolution of the Board of the National Bank of Ukraine No. 23 "On Some Issues of Operation of Ukrainian Banks and Banking Groups". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/v0023500-22.

The Ukrainian model of regulatory and legal oversight of the banking system is a comprehensive national framework that brings together institutional, prudential, stabilisation and ancillary regulatory components. The legislative level defines the general institutional framework and basic rules for the functioning of the banking sector, whilst the NBU's regulatory acts provide for the functional specification of supervisory and prudential requirements. This structural framework indicates that Ukrainian banking regulation is systematic in nature and covers not only banking activities themselves, but also the associated institutional, stabilisation and control mechanisms. At the same time, certain areas of banking regulation differ from EU law and require further harmonisation, particularly in relation to capital requirements, risk management, supervisory reporting, corporate governance, deposit guarantees, bank crisis resolution mechanisms, financial monitoring, digital operational resilience and cybersecurity.

The model of legal regulation of the EU banking system outlined in this study is consistent with the approaches set out in the academic literature, according to which EU banking law functions as a coherent, multi-level system in which prudential requirements and supervisory mechanisms are integrated within a common institutional framework. This conclusion is consistent with the position of A. Thomadakis & J. Arnal (2024), noting that the Single Supervisory Mechanism has evolved into a mature system with harmonised and transparent supervisory practices, whilst retaining the need for further adaptation to digital, climate and geopolitical challenges. At the same time, a study by P. Schammo (2021) argues that the formation of the Single Supervisory Mechanism is a manifestation of a more substantial institutional change within the European Banking Union, encompassing the redistribution of competences, powers and governance mechanisms between the supranational and national levels. This correlates with the aforementioned description of the EU banking regulation model, within which supervision is organised as a multi-level system combining supranational and national elements. T. Beck *et al.* (2023), in turn, justify the economic rationale for supranational banking supervision as a response to the limitations of fragmented national control models, which, in an integrated financial space, prove insufficient for proper risk management. This approach is consistent with the description provided of the institutional model of banking supervision in the EU, within which the supranational level is combined with the involvement of national regulators.

The findings of the study established that modern EU banking law goes beyond traditional prudential regulation and encompasses financial monitoring, digital operational resilience and cybersecurity as interrelated elements of a unified system for ensuring the resilience of the banking sector. This is consistent with the work of A. Minto & T. de Arruda (2026), noting that the creation of a new European Anti-Money Laundering Authority signals the EU's transition to a new level of institutional centralisation in the field of financial monitoring. The authors demonstrated that this is not merely about the emergence of a new regulator, but about a shift in the very approach to the application of national legislation, under which anti-money laundering mechanisms are increasingly being integrated into a single supranational system of coordination, control and the enforcement of uniform standards.

D. Clausmeier (2023) found that the Digital Operational Resilience Act (DORA) establishes digital operational resilience as a distinct area of EU financial regulation, within which information and communication technology risks, cyber threats and dependence on external digital suppliers are no longer viewed as a technical ancillary issue, but as a component of the overall supervisory assessment of financial institutions. This is consistent with the findings of the study, according to which financial monitoring, digital operational resilience and cybersecurity in EU law are integrated into a comprehensive model of banking regulation. Thus, EU banking law constitutes a systematically organised, multi-tiered regulatory model, within which prudential, supervisory, crisis management and related mechanisms are designed to ensure the stability of the banking sector. In contrast, the Ukrainian model is national in nature and is based on a combination of framework laws and regulatory provisions issued by the NBU.

The specifics of harmonising Ukrainian banking legislation with EU law

The harmonisation of Ukraine's banking legislation with EU law should be considered a consistent legal process aimed not only at updating individual provisions, but also at aligning the national model of banking regulation with European approaches in the areas of supervision, capital, internal governance, reporting, financial monitoring and digital resilience. In this sense, it forms part of the broader European integration of Ukraine's financial sector, rather than merely a technical exercise in adopting individual legal provisions. The contractual basis for this process is the Association Agreement between the European Union and its Member States, of the one part[1], and Ukraine, of the other part, which establishes a regulatory mechanism for the gradual alignment of Ukrainian legislation with EU law, particularly in the field of financial services. Therefore, the harmonisation of banking legislation is not

[1] Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. (2014, June). Retrieved from https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj/eng.

discretionary but mandatory in nature and is conducted within the framework of Ukraine's international legal obligations.

The institutional dimension of harmonisation relates to the role of the National Bank of Ukraine, which, in accordance with Law of Ukraine No. 679-XIV[1], combines the functions of a central bank, a banking regulatory body, a banking supervisory authority and a rule-making body. The NBU is responsible for the implementation of a significant part of the practical alignment of national banking regulation with EU standards, as the regulator specifies prudential, supervisory and organisational requirements for banks within the framework of its regulatory acts. The screening of financial services legislation lends further significance to this process. The National Bank of Ukraine's (2025) assessment of the alignment of national financial services legislation with the EU acquis, conducted as part of the screening process, demonstrated that the harmonisation of Ukraine's banking legislation has taken on not only an internal reformist character but also an externally assessed one in the context of Ukraine's preparations for EU accession.

The alignment of Ukrainian banking legislation with EU law takes two main forms. The first involves adapting laws and subordinate legislation to the content of EU directives and regulations, whilst the second involves specifying requirements regarding capital, risk management, internal capital adequacy assessment, supervisory reporting and corporate governance through NBU regulations. Therefore, the level of harmonisation is determined not only by laws but also by the NBU's regulatory practice. A separate area of focus is the introduction of a risk-based approach to banking supervision. This involves a shift from formal compliance with regulatory standards to an assessment of a bank's risk profile, the quality of its internal governance and its ability to maintain stability in a changing environment. In this respect the Ukrainian model aligns with the proposed approach to banking supervision in the EU, as set out in Directive 2013/36/EU of the European Parliament and of the Council[2], Regulation (EU) No. 575/2013 of the European Parliament and of the Council[3], as well as in the National Bank of Ukraine's national acts, in particular Resolution of the National Bank of Ukraine No. 64[4] and Resolution of the National Bank of Ukraine No. 161[5].

Convergence with EU law is also occurring through the gradual harmonisation of standards relating to capital, reporting, risk management and corporate governance. This means that a bank is viewed not merely as a subject of formal supervision, but as an institution that must continually demonstrate its resilience through its internal organisation, capital structure, disclosure of information and accountability to the supervisory authority. In EU law, these approaches are reflected in European Commission Implementing Regulation No. 2024/3117[6], Regulation of the European Parliament and the Council of the European Union No. 2024/1623[7], and in Ukrainian law – in Resolution of the National Bank of Ukraine No. 196[8], Resolution of the National Bank of Ukraine No. 64[9]and Decision of the National Bank of Ukraine No. 814-rsh[10]. In addition, harmonisation extends to related areas – anti-money laundering, data protection, digital operational resilience and cybersecurity – which is related to Regulation of the European Parliament and the Council of the European Union No. 2024/1620[11], Regulation of

[1] Law of Ukraine No. 679-XIV "On the National Bank of Ukraine". (1999, May). Retrieved from https://bank.gov.ua/en/legislation/Law_NBU.
[2] Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/dir/2013/36/oj/eng.
[3] Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms (Capital Requirements Regulation, CRR)". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/575/oj/eng.
[4] Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups". (2018, June). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_11062018_64.
[5] Resolution of the National Bank of Ukraine No. 161 "On Approval of the Regulation on Organization of Internal Capital Adequacy Assessment Process (ICAAP) in Banks of Ukraine and Banking Groups". (2021, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_30122021_161.
[6] European Commission Implementing Regulation No. 2024/3117 "Laying Down Implementing Technical Standards for the Application of Regulation (EU) No. 575/2013 of the European Parliament and of the Council with Regard to Supervisory Reporting of Institutions". (2024, November). Retrieved from https://eur-lex.europa.eu/eli/reg_impl/2024/3117/oj/eng.
[7] Regulation of the European Parliament and the Council of the European Union No. 2024/1623 "Amending Regulation (EU) No. 575/2013 as Regards Requirements for Credit Risk, Credit Valuation Adjustment Risk, Operational Risk, Market Risk and the Output Floor". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1623/oj/eng.
[8] Resolution of the National Bank of Ukraine No. 196 "On Approval of the Regulation on the Procedure for Determining the Regulatory Capital by Ukrainian Banks". (2023, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_28122023_196.
[9] Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups". (2018, June). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_11062018_64.
[10] Decision of the National Bank of Ukraine No. 814-rsh "On Approval of the Methodological Recommendations on Organization of Corporate Governance in Banks of Ukraine". (2018, December). Retrieved from https://bank.gov.ua/ua/legislation/Decision_03122018_814-rsh.
[11] Regulation of the European Parliament and the Council of the European Union No. 2024/1620 "Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng.

the European Parliament and the Council of the European Union No. 2024/1624[1], Directive of the European Parliament and the Council of the European Union No. 2024/1640[2], Regulation of the European Parliament and the Council of the European Union No. 2016/679[3], Regulation European Parliament and the Council of the European Union No. 2022/2554[4] and Directive of the European Parliament and the Council of the European Union No. 2022/2555[5]. In Ukraine, these areas are regulated by Law of Ukraine No. 361-IX[6], Law of Ukraine No. 2297-VI[7] and Law of Ukraine No. 2163-VIII[8]. This indicates that the Ukrainian model of alignment with EU law is no longer confined to narrow prudential regulation, but is gradually adopting an approach that treats the banking system as a sphere of comprehensive regulatory stability.

Despite significant progress, there are objective limits to the alignment of Ukrainian banking legislation with EU law. The main one relates to the difference between substantive and institutional harmonisation: Ukraine can align substantive rules on capital, reporting, risk management, depositor protection, financial monitoring and digital resilience, but cannot replicate the EU's supranational banking supervision architecture outside the scope of membership. This applies firstly to the Single Supervisory Mechanism, established by Council Regulation No. 1024/20130[9], and Regulation of the European Parliament and the Council of the European Union No. 806/2014[10], as well as approaches to the recovery and resolution of banks, as defined Directive of the European Parliament and the Council of the European Union No. 2014/59/EU[11]. They operate within a specific supranational institutional framework involving the European Central Bank and banking crisis resolution authorities. Consequently, these mechanisms can serve as a benchmark for Ukraine in terms of procedures, principles and the substance of regulation, but should not be replicated directly as institutional models.

In this regard, the harmonisation of Ukraine's banking legislation with EU law is primarily functional in nature: it aims to achieve results commensurate with European standards, even whilst preserving the national institutional framework. An additional constraint on harmonisation is the development of banking law under martial law, where adaptation to EU law must be balanced against the need to ensure the continuity of the banking system's operations and its resilience to exceptional risks. The harmonisation of Ukraine's banking legislation with EU law is a multi-level process encompassing international legal obligations, the activities of the NBU, and the updating of laws and subordinate legislation. At the same time, this process remains functional rather than entirely institutional, as Ukraine can align the substance and methods of banking regulation with EU law, but cannot fully replicate the supranational model of the European Banking Union.

In view of this, the subsequent analysis emphasises not a formal comparison of regulatory levels, but a categorical, substantive and functional comparison of the relevant elements of both models across key functional blocks. This identified not only the common and distinctive features of the relevant elements of legal regulation, but also determined which of them are most relevant for the further harmonisation of Ukrainian legislation with EU law (Table 2).

[1] Regulation of the European Parliament and the Council of the European Union No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng.

[2] Directive of the European Parliament and the Council of the European Union No. 2024/1640 "On the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng.

[3] Regulation of the European Parliament and the Council of the European Union No. 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)". (2016, April). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/eng.

[4] Regulation European Parliament and the Council of the European Union No. 2022/2554 "On Digital Operational Resilience for the Financial Sector". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[5] Directive of the European Parliament and the Council of the European Union No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive)". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[6] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20?lang=en.

[7] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en.

[8] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.

[9] Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions". (2013, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/1024/oj/eng.

[10] Regulation of the European Parliament and the Council of the European Union No. 806/2014 "Establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund". (2014, July). Retrieved from https://eur-lex.europa.eu/eli/reg/2014/806/oj/eng.

[11] Directive of the European Parliament and the Council of the European Union No. 2014/59/EU "Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms". (2014, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/59/oj/eng.

Table 2. A comparative analysis of the legal regulation of banking activities in the EU and Ukraine

Functional unit	EU	Ukraine	Common features	Differences	Relevance for further coordination
Prudential regulation	Uniform requirements regarding capital, liquidity, large exposures, internal governance and disclosure, as established in the Directive of the European Parliament and the Council of the European Union No. 2013/36/EU, Regulation European Parliament and the Council of the European Union No. 575/2013, Directive of the European Parliament and the Council of the European Union No. 2024/1619 and Regulation of the European Parliament and the Council of the European Union No. 2024/1623	The framework legislation and the detailed requirements in the Law of Ukraine No. 2121-III "On Banks and Banking", Resolution of the National Bank of Ukraine No. 196, Resolution of the National Bank of Ukraine No. 64 and Resolution of the National Bank of Ukraine No. 161	In both models, capital, liquidity and risk management are legal instruments for ensuring the bank's stability, as follows from the Directive of the European Parliament and the Council of the European Union No. 2013/36/EU, Regulation European Parliament and the Council of the European Union No. 575/2013, Law of Ukraine No. 2121-III "On Banks and Banking" and Resolution of the National Bank of Ukraine No. 196, Resolution of the National Bank of Ukraine No. 64	In the EU, prudential requirements are integrated into a single regulatory framework, whereas in Ukraine a significant proportion of the requirements are specified in secondary legislation issued by the NBU	Provisions relating to capital requirements, credit, market and operational risk, internal assessment of a bank's capital adequacy, supervisory review, environmental, social and governance risks, and the lower limit for calculating capital requirements require further harmonisation
Banking supervision	A multi-tiered supervisory system involving the European Central Bank and national competent authorities, established Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions" and Directive of the European Parliament and the Council of the European Union No. 2013/36/EU	The NBU's centralised national banking supervision following the Law of Ukraine No. 679-XIV "On the National Bank of Ukraine" and Law of Ukraine No. 2121-III "On Banks and Banking"	In both models, banking supervision is governed by public law and aims to ensure the stability of the banking system and protecting depositors	In the EU, supervision combines supranational and national levels, whereas in Ukraine, powers are concentrated primarily at the level of the NBU	It would be advisable to harmonise not the institutional model of the Single Supervisory Mechanism, but its functional elements: procedures for risk assessment, supervisory intervention, coordination and the application of a risk-based approach
Risk management and corporate governance	Requirements regarding internal management, control, governing bodies and risk assessment, stipulated by the Directive of the European Parliament and the Council of the European Union No. 2013/36/EU	Risk management and corporate governance regulated by the Law of Ukraine No. 2121-III "On Banks and Banking", Resolution of the National Bank of Ukraine No. 64, Resolution of the National Bank of Ukraine No. 161 and Decision of the National Bank of Ukraine No. 814-rsh	Both systems provide for internal controls, risk management, accountability of the bank's management bodies and the assessment of the risk profile	In the EU, these elements are incorporated into a standardised supervisory assessment, whereas in Ukraine they are largely set out in detail in NBU regulations and implemented through supervisory practice	Provisions relating to internal governance, risk appetite, the role of the supervisory board, internal control, stress testing and the bank's internal capital adequacy assessment require further coordination
Regulatory reporting	Reporting is a tool for standardising data within the single supervisory area in accordance with Regulation European Parliament and the Council of the European Union No. 575/2013 and European Commission Implementing Regulation No. 2024/3117	Reporting is used as a tool for national supervisory control in accordance with Resolution of the National Bank of Ukraine No. 120	In both models, reporting provides the information basis for banking supervision and risk management	In the EU, reporting ensures the comparability of data within a common supervisory framework, whereas in Ukraine it is primarily of internal regulatory significance	The methodology for supervisory reporting requires further harmonisation, particularly with regard to standardised reporting formats, data comparability and the use of reports in supervisory assessments

Table 2, Continued

Functional unit	EU	Ukraine	Common features	Differences	Relevance for further coordination
Depositor protection and insolvency resolution	A comprehensive system for recovery, early intervention, the resolution of banking crises, loss sharing and deposit guarantees is stipulated by the Directive of the European Parliament and the Council of the European Union No. 2014/59/EU, Regulation of the European Parliament and the Council of the European Union No. 806/2014 та Directive of the European Parliament and the Council of the European Union No. 2014/49/EU	Protection of depositors and the removal of insolvent banks from the market are regulated Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits"	Both models are designed to protect depositors, maintain confidence in the banking system and respond to bank failures	The EU has a systematically integrated crisis management mechanism in place, covering recovery, early intervention, resolution and the use of an internal loss-absorption tool, whereas in Ukraine the dominant approach is based on deposit guarantees and the withdrawal of banks from the market	Provisions relating to recovery plans, early intervention, resolution tools, internal loss absorption, crisis response coordination and deposit guarantee standards require harmonisation
Financial monitoring	A risk-based approach and a trend towards centralising control are stipulated by Regulation of the European Parliament and the Council of the European Union No. 2024/1620, Regulation of the European Parliament and the Council of the European Union No. 2024/1624 та Directive of the European Parliament and the Council of the European Union No. 2024/1640	The risk-based approach within the national financial monitoring system is provided for in Law of Ukraine No. 361-IX "On the Prevention and Countering of Money Laundering, Terrorist Financing and the Financing of the Proliferation of Weapons of Mass Destruction"	Both systems provide for customer identification, the assessment of high-risk transactions and the obligation for banks to conduct internal financial monitoring	In the EU, financial monitoring is increasingly being integrated into a supranational system of coordination and control, whereas in Ukraine it remains a nationally organised system	There is a need to harmonise approaches to customer due diligence, enhanced due diligence, beneficial ownership, data retention, reporting of suspicious transactions and supervisory coordination in the field of anti-money laundering and counter-terrorist financing
Data protection, digital operational resilience, cybersecurity	Protection of personal data, digital operational resilience and cybersecurity are regulated Regulation of the European Parliament and the Council of the European Union No. 2016/679, Regulation European Parliament and the Council of the European Union No. 2022/2554[1] and Directive of the European Parliament and the Council of the European Union No. 2022/2555	In Ukraine, the relevant sectors are covered by the Law of Ukraine No. 2297-VI "On Protection of Personal Data"[2] and Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine"	Both models acknowledge the impact of digital, information and cyber risks on the stability of the banking system	In the EU, digital operational resilience is a separate component of financial regulation and supervisory assessment, whereas in Ukraine these issues are regulated in a more piecemeal manner and are not fully integrated into banking supervision	There is a need to harmonise approaches to information and communication technology risk management, incident reporting, digital operational resilience testing, oversight of external digital suppliers, and the cybersecurity of critical entities

Source: compiled by the author based on Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions"[3], Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms"[4], Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms (Capital Requirements Regulation, CRR)"[5], Regulation of the European

[1] Regulation European Parliament and the Council of the European Union No. 2022/2554 "On Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[2] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en.

[3] Council Regulation No. 1024/2013 "Conferring Specific Tasks on the European Central Bank Concerning Policies Relating to the Prudential Supervision of Credit Institutions". (2013, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/1024/oj/eng.]

[4] Directive of the European Parliament and the Council of the European Union No. 2013/36/EU "On Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/dir/2013/36/oj/eng.

[5] Regulation European Parliament and the Council of the European Union No. 575/2013 "On Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No. 648/2012 (Capital Requirements Regulation, CRR)". (2013, June). Retrieved from https://eur-lex.europa.eu/eli/reg/2013/575/oj/eng.

Parliament and the Council of the European Union No. 806/2014 "Establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund"[1], Directive of the European Parliament and the Council of the European Union No. 2014/59/EU "Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms"[2], Directive of the European Parliament and the Council of the European Union No. 2014/49/EU "On Deposit Guarantee Schemes (Recast)"[3], Regulation of the European Parliament and the Council of the European Union No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)"[4], Regulation European Parliament and the Council of the European Union No. 2022/2554 "On Digital Operational Resilience for the Financial Sector"[5], Directive of the European Parliament and the Council of the European Union No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 (NIS 2 Directive)"[6], European Commission Implementing Regulation No. 2024/3117 "Laying Down Implementing Technical Standards for the Application of Regulation (EU) No. 575/2013 of the European Parliament and of the Council with Regard to Supervisory Reporting of Institutions and Repealing Commission Implementing Regulation (EU) 2021/451"[7], Directive of the European Parliament and the Council of the European Union No. 2024/1619 "Amending Directive 2013/36/EU as Regards Supervisory Powers, Sanctions, Third-Country Branches, and Environmental, Social and Governance Risks"[8], Regulation of the European Parliament and the Council of the European Union No. 2024/1623 "Amending Regulation (EU) No. 575/2013 as Regards Requirements for Credit Risk, Credit Valuation Adjustment Risk, Operational Risk, Market Risk and the Output Floor"[9], Regulation of the European Parliament and the Council of the European Union No. 2024/1620 "Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism"[10], Regulation of the European Parliament and the Council of the European Union No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing"[11], Directive of the European Parliament and the Council of the European Union No. 2024/1640 "On the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing"[12], Law of Ukraine No. 2121-III "On Banks and Banking"[13], Law of Ukraine No. 679-XIV "On the National Bank of Ukraine"[14], Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits"[15], Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of

[1] Regulation of the European Parliament and the Council of the European Union No. 806/2014 "Establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No. 1093/2010". (2014, July). Retrieved from https://eur-lex.europa.eu/eli/reg/2014/806/oj/eng.

[2] Directive of the European Parliament and the Council of the European Union No. 2014/59/EU "Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms and Amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No. 1093/2010 and (EU) No. 648/2012". (2014, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/59/oj/eng.

[3] Directive of the European Parliament and the Council of the European Union No. 2014/49/EU "On Deposit Guarantee Schemes (Recast)". (2014, April). Retrieved from https://eur-lex.europa.eu/eli/dir/2014/49/2014-07-02/eng.

[4] Regulation of the European Parliament and the Council of the European Union No. 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)". (2016, April). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/eng.

[5] Regulation European Parliament and the Council of the European Union No. 2022/2554 "On Digital Operational Resilience for the Financial Sector". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[6] Directive of the European Parliament and the Council of the European Union No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive)". (2022, December). Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[7] European Commission Implementing Regulation No. 2024/3117 "Laying Down Implementing Technical Standards for the Application of Regulation (EU) No. 575/2013 of the European Parliament and of the Council with Regard to Supervisory Reporting of Institutions and Repealing Commission Implementing Regulation (EU) 2021/451". (2024, November). Retrieved from https://eur-lex.europa.eu/eli/reg_impl/2024/3117/oj/eng.

[8] Directive of the European Parliament and the Council of the European Union No. 2024/1619 "Amending Directive 2013/36/EU as Regards Supervisory Powers, Sanctions, Third-Country Branches, and Environmental, Social and Governance Risks". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2024/1619/oj/eng.

[9] Regulation of the European Parliament and the Council of the European Union No. 2024/1623 "Amending Regulation (EU) No. 575/2013 as Regards Requirements for Credit Risk, Credit Valuation Adjustment Risk, Operational Risk, Market Risk and the Output Floor". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1623/oj/eng.

[10] Regulation of the European Parliament and the Council of the European Union No. 2024/1620 "Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng.

[11] Regulation of the European Parliament and the Council of the European Union No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng.

[12] Directive of the European Parliament and the Council of the European Union No. 2024/1640 "On the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng.

[13] Law of Ukraine No. 2121-III "On Banks and Banking". (2000, December). Retrieved from https://zakon.rada.gov.ua/go/2121-14?lang=en.

[14] Law of Ukraine No. 679-XIV "On the National Bank of Ukraine". (1999, May). Retrieved from https://bank.gov.ua/en/legislation/Law_NBU.

[15] Law of Ukraine No. 4452-VI "On the System of Guaranteeing Natural Person Deposits". (2012, February). Retrieved from https://zakon.rada.gov.ua/laws/show/4452-17?lang=en.

Weapons of Mass Destruction"[1], Law of Ukraine No. 2297-VI "On Protection of Personal Data"[2], Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine"[3], Resolution of the National Bank of Ukraine No. 196 "On Approval of the Regulation on the Procedure for Determining the Regulatory Capital by Ukrainian Banks"[4]; Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups"[5], Resolution of the National Bank of Ukraine No. 161 "On Approval of the Regulation on Organization of Internal Capital Adequacy Assessment Process (ICAAP) in Banks of Ukraine and Banking Groups"[6], Resolution of the National Bank of Ukraine No. 120 "On Approval of the Rules of Management of Statistical Reporting Filed with the NBU"[7], Decision of the National Bank of Ukraine No. 814-rsh "On Approval of the Methodological Recommendations on Organization of Corporate Governance in Banks of Ukraine"[8], Resolution of the Board of the National Bank of Ukraine No. 23 "On Some Issues of Operation of Ukrainian Banks and Banking Groups"[9]

The EU and Ukrainian models are characterised by functional similarities, which are evident in criteria such as regulatory objectives, risk management tools and the role of supervisory mechanisms: in both cases, legal regulation is aimed at ensuring the stability of the banking system, risk control, depositor protection and the consideration of related non-financial risks. At the same time, the differences are determined not only by the institutional level of supervisory organisation, but also by the degree of internal consistency within individual regulatory blocks.

The application of a systemic-structural approach has shown that, in EU law, the prudential, supervisory, crisis management and digital strands form an integrated model, within which supervisory procedures, crisis resolution mechanisms and risk management requirements constitute a coherent system for ensuring financial stability. In Ukraine, the relevant elements are also in place, but their interaction is less integrated and is implemented through a combination of framework laws, NBU regulations and specific mechanisms. Such discrepancies indicate that the main obstacle to further alignment of Ukrainian banking legislation with EU law is not only the absence of specific regulatory decisions, but also the insufficient integration of individual regulatory blocks into a coherent model of banking supervision and crisis response. At the same time, the identified substantive similarities in prudential regulation, risk management, supervisory reporting and financial monitoring lay the groundwork for further functional alignment of the Ukrainian model with EU law, whereas the most notable differences relate to anti-crisis regulation, the organisation of supervision, and the integration of digital operational resilience and cyber risks into banking supervision. This confirms that the implementation of the EU acquis in the banking sector in Ukraine is selective and functional in nature: certain elements already reflect the substance of European standards, whilst their systematic integration into a coherent regulatory model remains incomplete.

The findings of this comparative legal analysis not only identified the similarities and differences in the regulation of banking activities in the EU and Ukraine, but also interpreted them in the broader context of contemporary academic approaches to the functioning of banking regulation. The comparison of the identified patterns with the provisions of European doctrine makes it possible to assess the degree of consistency of the conclusions drawn with existing theoretical models and to clarify the nature and limits of the alignment of Ukrainian legislation with the EU acquis. In particular, the most pronounced substantive similarity, identified in the prudential block, requires separate academic consideration. This conclusion is consistent with the approach presented in the study by Y. Altunbaş *et al.* (2021), which demonstrates that the functioning of the Single Supervisory Mechanism influences practices regarding the disclosure of banking risks. A similar

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20?lang=en.

[2] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en.

[3] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.

[4] Resolution of the National Bank of Ukraine No. 196 "On Approval of the Regulation on the Procedure for Determining the Regulatory Capital by Ukrainian Banks". (2023, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_28122023_196.

[5] Resolution of the National Bank of Ukraine No. 64 "On Approval of the Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups". (2018, June). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_11062018_64.

[6] Resolution of the National Bank of Ukraine No. 161 "On Approval of the Regulation on Organization of Internal Capital Adequacy Assessment Process (ICAAP) in Banks of Ukraine and Banking Groups". (2021, December). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_30122021_161.

[7] Resolution of the National Bank of Ukraine No. 120 "On Approval of the Rules of Management of Statistical Reporting Filed with the NBU". (2018, November). Retrieved from https://bank.gov.ua/ua/legislation/Resolution_13112018_120.

[8] Decision of the National Bank of Ukraine No. 814-rsh "On Approval of the Methodological Recommendations on Organization of Corporate Governance in Banks of Ukraine". (2018, December). Retrieved from https://bank.gov.ua/ua/legislation/Decision_03122018_814-rsh.

[9] Resolution of the Board of the National Bank of Ukraine No. 23 "On Some Issues of Operation of Ukrainian Banks and Banking Groups". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/v0023500-22.

emphasis can be found in the study by K. Mérő & Á. Tardos (2024) which highlights the close interconnection between banks' financial reporting and prudential regulation. In the European model, capital, risks, reporting and the internal organisation of a bank are viewed as interrelated elements of a single supervisory regime.

The study by J.A. Fernández Fernández (2023) addressed the European Banking Union as a complex, multi-level structure, the development of which is determined not only by formal rules but also by the internal interactions between its institutional elements. This approach corresponds to the characterisation of EU banking regulation presented in this study as a systemically organised model, within which prudential requirements, supervisory mechanisms, anti-crisis instruments and related control regimes function in an interrelated manner. C. Papathanassiou (2022) demonstrated that banking supervision in the EU has not only a technical but also a distinct legal dimension, as it is conducted within the broader EU legal order and cannot be considered in isolation from legal safeguards and general principles of law. This complements the characterisation of the European model of banking regulation as one that combines institutional, supervisory and legal elements within a single regulatory framework.

The findings of the study showed that, in the area of anti-money laundering, there is a close alignment between Ukrainian and EU law in the application of a risk-based approach. At the same time, the organisation of this area of regulation remains different: whilst in the EU the development of anti-money laundering measures is linked to increased supranational coordination, in Ukraine the relevant mechanism retains a predominantly national character. This is consistent with the study by S. Tosza & O. Voordeckers (2024), in which the creation of a new European body in the field of anti-money laundering is viewed as a shift of the centre of gravity to the supranational level. Thus, in this area, there is a similarity in the regulatory approach between Ukraine and the EU, but not an identity of the institutional model.

The study by E. Carletti *et al.* (2021) shows that supervision within the European Banking Union is based on a specific system of interaction between the central and national levels, in which the effectiveness of supervision depends not only on the formal division of powers, but also on the quality of information exchange and coordination between participants in the supervisory process. J. Zeitlin (2023) characterised the Single Supervisory Mechanism as a multi-level structure combining elements of hierarchy, coordination and flexible governance. In the study by M. Božina Beroš (2023), the emphasis is placed on the fact that the EU's common supervisory model is shaped through constant interaction between supranational and national authorities, as well as through the development of a common supervisory culture. Taken together, these authors' works are consistent with the findings of the present study, according to which the Ukrainian model corresponds to EU law primarily in a functional rather than an institutional dimension. Ukraine can align the content of regulation, supervisory procedures and control methods with EU standards; however, the supranational architecture of the European Banking Union cannot be replicated outside the EU.

The findings of the study revealed that differences remain between EU law and Ukrainian legislation in the area of bank insolvency resolution and depositor protection. The element of the Ukrainian model most comparable to EU law is the deposit guarantee scheme, whereas the mechanisms for early intervention, the restoration of banking operations and the resolution of banking crises in Ukrainian law have not yet attained the systematic nature characteristic of the European model. At the same time, T.F. Huertas (2022) argued that the system for resolving banking crises and deposit guarantees in the Eurozone is not yet complete and requires further review to ensure a more consistent and effective response to banking crises. The author emphasised the need for better coordination of crisis resolution mechanisms, loss allocation and depositor protection, as the fragmentation of these elements undermines the integrity of the anti-crisis model. The study by M. Tümmler (2022) demonstrated that the development of a common European deposit insurance scheme is hampered not only by economic considerations but also by institutional and political factors linked to the positions of Member States and the role of national deposit guarantee schemes. This confirms the conclusion of this study that the anti-crisis bloc is one of the most complex areas for further harmonisation of Ukrainian banking legislation with EU law.

The differences between the Ukrainian and European models in the area of depositor protection and bank insolvency resolution identified in the present study are consistent with the approach taken by V. Krahlevych (2022), who argues for the need to further align the national deposit guarantee scheme with EU standards. At the same time, the conclusion that the alignment of Ukraine's banking legislation with EU law is already occurring at the level of individual regulatory institutions is consistent with the position of V.V. Skryl (2023), according to which the integration of Ukraine's banking system into the European banking area is already finding practical expression in certain segments of financial regulation. The approach to harmonisation as an uneven and not yet fully completed process is consistent with the findings of P.S. Patsurkivskyi & R.O. Havryliuk (2025), who emphasised the more comprehensive yet still fragmentary nature of the implementation of EU financial law in Ukraine. In turn, the conclusion regarding the limitations of a full institutional replication of the European model of banking supervision corresponds with the study by A. Demianiuk (2025), which focuses on the institutional and regulatory features

of the organisation of supervision in Ukraine and the EU. Consequently, further harmonisation of Ukrainian legislation with EU law is most realistic in functional terms – through the adoption of supervisory procedures, approaches and standards, rather than through the direct replication of the supranational model of the European Banking Union.

The findings of the study revealed that the greatest differences between Ukrainian legislation and EU law persist in the areas of digital operational resilience, cybersecurity and the incorporation of digital risks into banking supervision. This is consistent with the findings of C. Buttigieg & B.B. Zimmermann (2024), who demonstrated that the EU regulation on digital operational resilience creates a harmonised framework for regulating the digital resilience of the financial sector, but at the same time highlights issues of fragmented supervision, inconsistent national approaches and insufficient coordination within the European financial supervisory system. The Ukrainian model has not yet reached the level of integration of new digital and related risks into banking supervision that is already taking shape in EU law; consequently, this area remains one of the priority areas for further adaptation.

Consequently, the further alignment of Ukraine's banking legislation with EU law requires not only the updating of specific regulatory provisions, but also the strengthening of systemic coherence between the main functional areas of banking regulation. Priorities in this context include improving mechanisms for responding to bank insolvency, standardising supervisory reporting, integrating financial monitoring into the overall banking supervision system, and incorporating digital operational resilience and cyber risks into the comprehensive supervisory assessment of banks. The effectiveness of this process will depend not only on the pace of updating the regulatory framework but also on the ability to ensure its systematic and consistent implementation.

Conclusions

The findings of the study showed that the legal regulation of the EU banking system operates as a coherent, multi-tiered system in which prudential requirements, supervisory mechanisms, crisis management tools and related control regimes form a unified framework for ensuring financial stability. The Ukrainian model of banking regulation is based on a combination of framework laws and NBU regulations, which provide detailed requirements for capital, risk management, reporting and corporate governance. The alignment of Ukraine's banking legislation with EU law is mandatory and is conducted within the framework of the state's international legal obligations and the NBU's practical rule-making activities. The most pronounced similarity in substance is evident in prudential regulation, where Ukrainian legislation most consistently reflects European approaches to capital adequacy, internal control, risk assessment and supervisory procedures. Supervisory reporting in Ukraine, despite its standardisation, has not yet reached the level of unification and comparability characteristic of the EU's single supervisory area. In the area of depositor protection, Ukrainian law has established an independent and relatively well-developed mechanism; however, in terms of early intervention, the restoration of banking operations and crisis resolution, it still behind the systematic nature of the European model. In the area of anti-money laundering, Ukrainian legislation is similar to European legislation in its approach, yet it retains a predominantly national framework for supervision, whereas EU law shows a trend towards greater centralisation.

The most notable differences between Ukraine and the EU lie in the areas of digital operational resilience, cybersecurity and data protection, which, in the European model, are already integrated into the banking supervision system as components of a bank's resilience assessment. At the same time, the further alignment of Ukrainian legislation with EU law is primarily of a functional nature, as it primarily involves bringing the content of regulation, supervisory procedures and control methods into line with European standards. In the absence of EU membership, the Ukrainian legal system cannot replicate the supranational architecture of the European Banking Union; therefore, the full institutional replication of the European model remains objectively limited. An additional factor influencing the pace and depth of this process is the need to combine adaptation to EU law with ensuring the continuity and stability of the banking system under martial law. At the same time, the key task remains ensuring internal consistency between the prudential, supervisory, anti-crisis and related strands of banking regulation.

Consequently, the further development of Ukraine's banking legislation should be directed not merely at updating individual provisions, but at systematically improving the entire model of banking regulation, particularly regarding reporting, crisis management mechanisms, digital resilience and the institutional capacity of supervisory authorities. Future research should conduct an in-depth examination of the practical impact of harmonising Ukraine's banking legislation with EU law on supervisory practice, the financial stability of the banking sector, the institutional capacity of banking supervisory authorities, and Ukraine's readiness for further European integration.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Altunbaş, Y., Polizzi, S., Scannella, E., & Thornton, J. (2021). European banking union and bank risk disclosure: The effects of the Single Supervisory Mechanism. *Review of Quantitative Finance and Accounting*, 58(3), 649-683. doi: 10.1007/s11156-021-01005-z.

[2] Beck, T., Silva-Buston, C., & Wagner, W. (2023). The economics of supranational bank supervision. *Journal of Financial and Quantitative Analysis*, 58(1), 324-351. doi: 10.1017/S0022109022000588.

[3] Božina Beroš, M. (2023). Developing banking union's common supervisory culture: A look into the "black box" of joint supervisory teams. *Journal of European Integration*, 45(1), 103-120. doi: 10.1080/07036337.2022.2156994.

[4] Buttigieg, C., & Zimmermann, B.B. (2024). The digital operational resilience act: Challenges and some reflections on the adequacy of Europe's architecture for financial supervision. *ERA Forum*, 25(1), 11-28. doi: 10.1007/s12027-024-00793-w.

[5] Carletti, E., Dell'Ariccia, G., & Marquez, R. (2021). Supervisory incentives in a banking union. *Management Science*, 67(1), 455-470. doi: 10.1287/mnsc.2019.3448.

[6] Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review*, 4, 79-90. doi: 10.1365/s43439-022-00076-5.

[7] de Groen, W.P. (2023). The banking union: Supervision and crisis management. In D. Adamski, F. Amtenbrink & J. de Haan (Eds.), *The Cambridge handbook of European monetary, economic and financial integration* (pp. 478-497). Cambridge: Cambridge University Press. doi: 10.1017/9781009364706.031.

[8] Demianiuk, A. (2025). *Banking supervision in Ukraine and the EU: A comparative legal analysis*. Kyiv: National University of Kyiv-Mohyla Academy.

[9] Dmytrenko, E. (2021). Peculiarities of legal regulation of banking relations in the conditions of Ukraine's European integration. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*, 8(3), 144-150. doi: 10.23939/law2021.31.144.

[10] Fernández Fernández, J.A. (2023). European Banking Union structures and dynamics. *Cogent Economics & Finance*, 11(2), article number 2256192. doi: 10.1080/23322039.2023.2256192.

[11] Huertas, T.F. (2022). Reset required: The Euro-area crisis management and deposit insurance framework. *Journal of Financial Regulation*, 8(2), 187-202. doi: 10.1093/jfr/fjac007.

[12] Hülsewig, O., & Steinbach, A. (2025). Banking regulation and sovereign default risk: How regulation undermines rules. *European Journal of Risk Regulation*. doi: 10.1017/err.2025.10041.

[13] Krahlevych, V. (2022). The Deposit Guarantee Fund of Ukraine: Towards EU standards of rights protection. *Academy of Economic and Environmental Studies*, 18(5), 135-144. doi: 10.33327/AJEE-18-5.4-n000430.

[14] Lamandini, M., D'Ambrosio, R., & Ramos Muñoz, D. (2022). Supervisory review and evaluation process (SREP) in the context of the exercise of supervisory powers and extraordinary measures. In *European banking law and regulation* (pp. 526-547). Oxford: Oxford University Press. doi: 10.1093/law/9780198867319.003.0018.

[15] Lo Schiavo, G. (2024). *EU banking law and regulation*. Oxford: Oxford University Press. doi: 10.1093/law/9780192864437.001.0001.

[16] Mérő, K., & Tardos, Á. (2024). Differences and interactions between banks' financial statements and prudential regulation. *Journal of Banking Regulation*, 26, 164-175. doi: 10.1057/s41261-024-00253-y.

[17] Minto, A., & de Arruda, T. (2026). The new EU anti-money laundering authority (AMLA) and the standard for the application of national laws: "What's past is prologue"? *European Business Organization Law Review*, 26, 689-718. doi: 10.1007/s40804-026-00360-5.

[18] National Bank of Ukraine. (2025). *NBU presents European Commission with assessment of harmonizing financial services national laws with EU acquis as part of screening*. Retrieved from https://bank.gov.ua/ua/news/all/natsionalniy-bank-u-mejah-skriningu-predstaviv-yevropeyskiy-komisiyi-otsinku-nablijennya-natsionalnogo-zakonodavstva-do-aktiv-prava-yes-v-sferi-finansovih-poslug.

[19] Papathanassiou, C. (2022). Fundamental rights and banking supervision. *Journal of Banking Regulation*, 24, 420-431. doi: 10.1057/s41261-022-00204-5.

[20] Parchimowicz, K. (2023). Banking regulation in Europe: From reaction to thinking ahead. In D. Adamski, F. Amtenbrink & J. de Haan (Eds.), *The Cambridge handbook of European monetary, economic and financial integration* (pp. 421-442). Cambridge: Cambridge University Press. doi: 10.1017/9781009364706.028.

[21] Patsurkivskyi, P.S., & Havryliuk, R.O. (2025). Implementation of the EU financial acquis by Ukraine. *Uzhhorod National University Herald. Series: Law*, 3(87), 102-111. doi: 10.24144/2307-3322.2025.87.3.15.

[22] Schammo, P. (2021). Institutional change in the Banking Union: The case of the Single Supervisory Mechanism. *Yearbook of European Law*, 40, 265-309. doi: 10.1093/yel/yeab002.

[23] Skryl, V.V. (2023). Integration of the banking system of Ukraine into the European banking community. In V. Skryl (Ed.), *Sustainable development: Challenges and threats in modern realities: Proceedings of the international scientific and practical internet conference* (pp. 132-133). Poltava: National University "Yuri Kondratyuk Poltava Polytechnic".
[24] Thomadakis, A., & Arnal, J. (2024). Ten years of the Single Supervisory Mechanism: Looking into the past, navigating into the future. *Journal of Financial Regulation*, 10(2), 253-258. doi: 10.1093/jfr/fjae005.
[25] Tosza, S., & Voordeckers, O. (2024). An anti-money laundering authority for the European Union: A new center of gravity in AML enforcement. *ERA Forum*, 25, 405-424. doi: 10.1007/s12027-024-00805-9.
[26] Tümmler, M. (2022). Completing banking union? The role of national deposit guarantee schemes in shifting member states' preferences on the European deposit insurance scheme. *Journal of Common Market Studies*, 60(6), 1556-1572. doi: 10.1111/jcms.13318.
[27] Vese, D. (2025). Discretion and the public interest: The case of the European Banking Authority. *Cambridge Law Journal*, 84(2), 368-396. doi: 10.1017/S0008197325100718.
[28] Zeitlin, J. (2023). Hierarchy, polyarchy, and experimentalism in EU banking regulation: The Single Supervisory Mechanism in action. *Journal of European Integration*, 45(1), 79-101. doi: 10.1080/07036337.2022.2144279.

Правове регулювання банківської системи України в умовах євроінтеграції: порівняльно-правовий аналіз із законодавством ЄС

Андрій Цвєтков

Кандидат юридичних наук, старший науковий співробітник
Науково-дослідний інститут приватного права і підприємництва
імені академіка Ф.Г. Бурчака Національної академії правових наук України
03150, вул. Казимира Малевича, 11, м. Київ, Україна
https://orcid.org/0000-0002-3239-322X

Анотація
Метою дослідження було зіставлення правового регулювання банківської системи України з європейськими правовими стандартами для окреслення напрямів його подальшого вдосконалення. Для цього були використані методи доктринально-правового, порівняльно-правового, системно-структурного аналізу. Результати дослідження засвідчили, що гармонізація банківського законодавства України з правом Європейського Союзу має нерівномірний характер. Найвиразніша змістова близькість між моделями простежується у пруденційному блоці та суміжних сферах управління ризиками, наглядової звітності й фінансового моніторингу, натомість найпомітніші відмінності стосуються антикризового регулювання, організації нагляду та інтеграції цифрової операційної стійкості й кіберризиків до банківського нагляду. В обох моделях правове регулювання спрямоване на забезпечення стійкості банківської системи, контроль за ризиками, захист вкладників і врахування суміжних нефінансових ризиків, зокрема у сферах фінансового моніторингу, захисту даних і кібербезпеки. Встановлено, що українська модель наближення до права Європейського Союзу має переважно функціональний характер, оскільки вона відображає зміст і методи європейського банківського регулювання, але не може повністю відтворити наднаціональну інституційну архітектуру Європейського банківського союзу. У зв'язку з цим подальше узгодження банківського законодавства України з правом Європейського Союзу пов'язане не лише з оновленням окремих норм, а й з посиленням системної узгодженості між пруденційним, наглядовим, антикризовим і цифровим блоками регулювання. Тому подальша адаптація законодавства України до права Європейського Союзу потребує уніфікації наглядової звітності, розвитку механізмів урегулювання банківських криз та інтеграції цифрової операційної стійкості. Практичне значення результатів полягає в можливості їх використання Національним банком України, органами державної влади та науково-освітніми установами для вдосконалення банківського законодавства, його адаптації до європейського права і в освітньому процесі

Ключові слова:
правове управління ризиками; регулювання фінансового моніторингу; гармонізація законодавства; правове партнерство держави та бізнесу; правова відповідальність; правове регулювання ринкових відносин

UDC 351.811
DOI: 10.63341/naia-chasopis/2.2026.62

ISSN 2519-4216
E-ISSN 2519-4313

Automated system for recording administrative offences in the field of road traffic safety

Olha Markiv
Chief Inspector
Department of Patrol Police of the National Police of Ukraine
03048, 3 Fedir Ernst Str., Kyiv, Ukraine
https://orcid.org/0009-0005-6453-7389

Olha Bychkova
Inspector
Main Directorate of the National Police in Odesa Region
65014, 12 Yevreiska Str., Odesa, Ukraine
https://orcid.org/0009-0008-7590-4721

Yevheniia Murzo*
Doctor of Philosophy in Law, Senior Investigator
Main Investigation Department of the National Police of Ukraine
01024, 10 Academician Bohomolets Str., Kyiv, Ukraine
https://orcid.org/0009-0000-4409-0560

Abstract
This study is motivated by the introduction of automatic traffic offence enforcement systems and the need to reconsider their legal, organisational, and procedural regulation in the context of digitalisation of public administration. The aim of this study was to examine the specifics of regulatory consolidation, organisation, and application of the system of automatic recording of traffic violations in Ukraine and individual states. The paper employed formal legal, systemic-structural, comparative legal, logical-semantic, and analytical methods. The study found that the regulatory framework governing the operation of the automatic recording system in Ukraine is formed by provisions of codified administrative legislation, governmental regulations, and departmental regulations, which together define the substantive, organisational, technical, and procedural foundations of its operation. It was revealed that the Ukrainian model is characterised by a specific legal definition of the liable person, issuance of a decision without drawing up a protocol and without the direct participation of the person in administrative proceedings. It was proven that the evidential base in cases of this category is formed by technical enforcement devices and data from official state registers, which determines the specific nature of procedural guarantees. It has been established that the enforcement stage of

Article's History:
Received: 16.01.2026
Revised: 10.04.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Markiv, O., Bychkova, O., & Murzo, Ye. (2026). Automated system for recording administrative offences in the field of road traffic safety. *Law Journal of the National Academy of Internal Affairs*, 16(2), 62-74. doi: 10.63341/naia-chasopis/2.2026.62.

*Corresponding author (*yevheniiamurzo@gmail.com*)

the administrative decision is of independent significance in ensuring proper notification of the individual and protection of procedural rights. Comparative analysis showed that in France, the United Kingdom, individual states of Australia, and New Zealand, automatic recording is combined with more developed mechanisms for technical approval of enforcement tools and the use of automatically obtained data as evidence. The study is of practical importance for the further development of the national model in terms of legal certainty, admissibility of automatically obtained data, technical suitability of control tools, and protection of personal data of road users

Keywords:
administrative liability; liable person; automated speed enforcement; evidential value of technical data; appeal of decision; personal data protection; comparative legal analysis

Introduction

Automatic recording of road violations is an important element of modern systems for ensuring safety in transport infrastructure and government policy in the field of road traffic. Contemporary scientific studies show that the introduction of technologies for automatic control of traffic violations, in particular, the recording of speeding and other offences using stationary and mobile complexes, in most cases is associated with a decrease in the number of road accidents and the severity of their consequences. In particular, in the systematic review, A. Alobaidallah *et al*. (2025) summarised the results of international studies that confirm the positive impact of automated control systems on road safety indicators, while emphasising the dependence of the effect on implementation models, public perception, and stability of law enforcement.

Similar results were obtained by C. Luca (2024), who stated that automatic control systems contribute to improving the discipline of road users, optimizing traffic flows, and improving the efficiency of traffic management in general. The study by M. Sebapalo *et al*. (2025), based on the material of the city of Gaborone (Botswana), according to experts in the field of transport and road safety, associated the use of cameras with curbing traffic violations and reducing accidents in their installation areas.

Quantitative empirical data also confirmed the positive safety impact of such systems. Thus, an analysis of the automatic speed control programme in New York showed that in areas where cameras were installed in 2022, in the subsequent period, there was a decrease in the number of injuries and deaths. In particular, the comparison of indicators for 2021-2023 allowed tracking the change in accidents before and after the installation of cameras: according to data (New York City Department of Transportation, 2024), the number of such cases was 14% lower compared to the control road corridors without cameras. Similar results were obtained in other studies: in the longitudinal analysis of the automatic speed enforcement programme in New York, J. Gao *et al*. (2025) recorded a statistically significant reduction in the number of road accidents after the installation of fixed cameras, while emphasising the unevenness and contextual dependence of this effect.

A separate area of contemporary research is devoted to the legal and organisational aspects of the functioning of automatic crime recording systems. In particular, A. Vadeby & C. Howard (2024) in a study of the effectiveness of the system of fixed speed cameras in Sweden found that their use contributes to increased compliance with the speed limit, a decrease in the average speed of vehicles, and is accompanied by a reduction in the number of deaths in road accidents. K. Shaaban *et al.* (2023), based on empirical data on the use of fixed speed cameras, proved that automatic systems contribute to reducing the speed of vehicles and increasing the level of compliance by drivers with the established speed limits. In turn Z. Cheng *et al.* (2025), based on longitudinal analysis of data on the installation of road cameras, found a statistically significant decrease in the number of road accidents after the introduction of automatic control systems. The researchers explained this effect by a combination of technical capabilities for automatic detection of violations, constant video surveillance, and a behavioural deterrent effect, which forms a more cautious model of behaviour on the road for drivers.

Despite a significant number of international studies, insufficient attention is paid to a comprehensive comparative analysis of the Ukrainian model of automatic recording of offences with approaches used in other countries. In particular, they require additional scientific understanding of the issues of legal regulation of the functioning of such systems, organisation of their application, and ensuring a balance between the effectiveness of control and guarantees of the rights of road users. In this regard, the relevance of the study is conditioned by the need for a critical analysis of the current state of regulatory support, organisation, and practice of using automatic crime detection systems as an important component of the national policy in the field of road safety.

The purpose of the study was to investigate the specific features of regulatory consolidation, organisation, and application of the system of recording traffic violations in automatic mode in Ukraine and individual states to determine the areas for further development of the national model in terms of legal certainty, the

permissibility of using automatically obtained data, the technical suitability of control tools, and ensuring the privacy of road users. To achieve this goal, the following research objectives were defined:

1) to analyse the regulatory framework for the functioning of systems for automatic recording of administrative offences in the field of road safety;

2) to investigate the organisational, technical, and procedural features of the application of the automatic recording system, in particular, regarding the determination of the responsible person, making a decision, the evidential value of technical data, the implementation of the decision and its appeal;

3) to comparatively analyse the Ukrainian model and approaches used in France, Great Britain, individual states of Australia, and New Zealand, to determine possible areas for improving national regulation and law enforcement practices.

Literature Review

The analysis of contemporary scientific literature gives grounds to identify several main areas of research of automated control systems in the field of road traffic. The first area covers works in which automatic recording is considered through the prism of its safety efficiency. In these studies, M. Delavary *et al*. (2024), Z. Cheng *et al*. (2025), and A.W. Howard *et al*. (2025) analysed the impact of speed cameras, cameras that record vehicles running red lights, automatic number plate recognition systems, and other technical measures on accident rates, the severity of road traffic accident consequences, and drivers' speed behaviour. A. Vadeby & C. Howard (2024), A. Alobaidallah *et al*. (2025), J. Gao *et al*. (2025), generally confirmed the positive impact of automated control on the discipline of road users, reducing speed violations, and road safety indicators. These studies showed that the effectiveness of such systems is not automatic or universal, but depends on the location of the cameras, traffic intensity, stability of law enforcement, the implementation model, and the level of public trust.

The second area is related to the investigation of behavioural and social effects of automated control. In this aspect, it is important to pay attention not only to reducing the number of violations, but also to how drivers adapt their behaviour to the presence of cameras. In particular, E.C. Amancio *et al*. (2024) investigated the effect of fixed speed cameras on the actual speed behaviour of drivers, whereas S.L. Valderrama *et al*. (2024) highlighted the possible behavioural side effects of automatic monitoring, in particular, changes in driver behaviour after driving through the area where the camera is installed. In the same context, S.A.A. Safavi-Naini *et al*. (2024), studying the behaviour of drivers when using fixed and sectional speed control cameras, showed that the effectiveness of such tools depends on the type of control and the behavioural response of drivers. Such studies allow critically evaluating automatic recording not as a self-contained tool, but as an element of a broader road safety policy. This is important for legal analysis, since the effectiveness of automatic recording cannot be evaluated solely by the number of decisions made or the number of technical means installed.

The next area concerns the public perception of automated control. A. Delbosc *et al*. (2025) showed that the maintenance of such systems depends not only on their actual effectiveness, but also on whether they are perceived as fair, transparent, and aimed specifically at security, and not at fiscal filling of the budget. For the Ukrainian context, this approach is particularly important, since automatic recording involves making a decision without drawing up a protocol and without the direct participation of a person at the initial stage of proceedings. In such circumstances, the legitimacy of the system depends on the clarity of the procedure, the availability of appeal mechanisms, and the actual ability of a person to refute the presumption of responsibility.

The fourth area covers the investigation of the legal limits of digital control, personal data protection, and the permissibility of using surveillance technologies. C. Slobogin & S. Brayne (2023) regards surveillance technologies as part of broader mechanisms of state control, which need to be assessed in terms of legality, proportionality, and the protection of privacy. Research on approaches to ensuring privacy-by-design stage of smart environments is of related importance, since automatic detection of offences functions within the broader digital infrastructure for data collection, processing, and use (Ivanovska *et al*., 2025). For automatic recording systems, this is of direct importance, since their operation is associated with the collection and processing of data about the vehicle, its registration number, place, time, and circumstances of the recorded event.

Thus, contemporary scientific literature comprehensively covers the effectiveness of automated control systems, their behavioural impact, public perception, and individual risks of digital surveillance. The question of how exactly the automatically obtained technical data is integrated into the legal procedure for bringing to administrative responsibility remains rather neglected. It is precisely this circumstance that determines the academic need to analyse automated enforcement not merely as a means of monitoring compliance with road traffic regulations, but as a specific administrative and procedural model, within which legal certainty, the evidential value of the data obtained, the technical suitability of the devices, the identification of the responsible person, appeals against decisions, and the protection of personal data must be mutually consistent.

Materials and Methods

The study of the system for recording administrative offences in the field of road safety in automatic mode was

carried out using administrative legal and comparative legal approaches. Conceptually, the research was based on the understanding of automatic recording not only as a technical method for detecting violations, but as a regulatory and procedurally regulated mechanism for implementing bringing to administrative responsibility, the functioning of which depends on a combination of substantive, evidential, procedural, and organisational and technical elements. This approach allowed investigating the relevant issues, both in the plane of legal regulation and in the plane of law enforcement.

The main research method employed was the formal legal approach, which was used to analyse the provisions of the Code of Ukraine on Administrative Offences[1], and subordinate legislation issued by the Cabinet of Ministers of Ukraine and the Ministry of Internal Affairs of Ukraine, which define the legal framework for the operation of the automatic recording system, the procedure for issuing decisions, the mechanisms for exemption from administrative liability, the enforcement of decisions, and the procedures for appealing against them. It was the application of this method that helped to establish the regulatory structure of the responsible person, find out the procedural features of administrative proceedings, and identify the specifics of the legal regime of automatically obtained data. The system structural method was used to analyse the internal construction of the model under study. With its help, the automatic recording system was considered as an integral mechanism, within which the regulatory framework, technical means of control, evidence base, the procedure for notifying a person, the implementation of a decision, and appeal mechanisms are interrelated. The functional significance of each of the elements in the overall structure of administrative and tort response was determined.

The comparative legal method was used to compare the Ukrainian model of automatic recording with individual approaches. In this context, official materials from France, the United Kingdom, the Australian states of Victoria and New South Wales, Sweden, and New Zealand (New Zealand Transport Agency, 2024; Observatoire National Interministeriel de la Securite Routiere, 2024; Vadeby & Howard, 2024; Department of Justice and Community Safety, 2025) were analysed. This method identified the features of technical approval of control tools, evidence-based use of automatically obtained data, organisational integration of automatic recording systems, and legal assessment of privacy risks.

Results

The normative legal basis for the functioning of the system of recording administrative offences in the field of road safety in automatic mode in Ukraine is established by the provisions of the Code of Ukraine on Administrative Offences, which defines the general principles of administrative responsibility and the specifics of proceedings in cases of offences recorded in automatic mode[2]. Organisational and technical aspects of the system's functioning are regulated by Resolution No. 833 of the Cabinet of Ministers of Ukraine dated November 10, 2017[3], which defines the procedure for implementing technical means (control devices), information processing, and interaction between subjects of power. The procedure for processing documents relating to administrative offences is governed by Order No. 13 of the Ministry of Internal Affairs of Ukraine dated 13 January 2020, which sets out the steps to be taken by authorised officials[4].

The introduction in Ukraine of the system of automatic recording of administrative offences in the field of road safety is considered as one of the priority areas of the government policy aimed at increasing the level of compliance by drivers with the established speed limits and reducing accident rates. As of June 2026, there were 376 stationary technical means (monitoring devices) in Ukraine that record violations of exceeding the established speed limits of vehicles (more than 20 km/h and more than 50 km/h), and violations of traffic rules and stops on lanes for route vehicles (Patrol Police Department of Ukraine, 2026). These measures are generally implemented in areas with a high concentration of road traffic accidents and on sections of motorways where there is a high risk of accidents.

The use of technical devices with photo and video recording functions is carried out in accordance with the Technical Regulations for Legally Regulated Measuring Instruments, approved by Resolution No. 94 of the Cabinet of Ministers of Ukraine dated 13 January 2016[5]. Within the framework of this regulation, such devices are classified as remote speed meters of vehicles and remote meters of spatial and temporal location parameters.

The lawful use of the specified technical equipment in the field of legally regulated metrology is ensured provided that all established requirements are fully complied with, in particular: compliance with the essential requirements of the Technical Regulation regarding metrological characteristics and data protection; compliance with the technical specifications set

[1] Code of Ukraine on Administrative Offences. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[2] Ibidem, 1984.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 833 "On Approval of the Procedure for the Functioning of the System for Recording Administrative Offences in the Field of Road Safety in Automatic Mode". (2017, November). Retrieved from https://zakon.rada.gov.ua/laws/show/833-2017-%D0%BF.
[4] Order of the Ministry of Internal Affairs of Ukraine No. 13 "On Approval of the Instruction on Processing Materials on Administrative Offences Recorded in Automatic Mode". (2020, January). Retrieved from https://zakon.rada.gov.ua/laws/show/z0113-20.
[5] Resolution of the Cabinet of Ministers of Ukraine No. 94 "Technical Regulation of Legally Regulated Measuring Instruments". (2016, January). Retrieved from https://zakon.rada.gov.ua/laws/show/94-2016-%D0%BF.

out in the national standard DSTU 8809:2018[1], which regulates maximum permissible measurement errors and software requirements; completion of the conformity assessment procedure and the possession of valid calibration certificates in accordance with the requirements of Law of Ukraine No. 1314-VII[2]. Thus, compliance with the established technical and metrological requirements is a necessary prerequisite for recognising the results of automatic recording as appropriate and acceptable evidence in cases of administrative offences.

As a result of the analysis of the procedural features of administrative proceedings, it was established that the specifics of this model consist in a special definition of the subject of administrative responsibility. According to the Code of Ukraine on Administrative Offences (CUAO)[3], the person liable for offences recorded in automatic mode is an individual or the head of the legal entity for which the vehicle is registered; a proper user of the vehicle, if the relevant information is entered in the Unified State Register of Vehicles; a person who performs the powers of the head of the legal entity, if there is no information about the head in the Unified State Register of Legal Entities, Individual Entrepreneurs, and Public Organisations at the time of the request. It was established that the legislative model actually establishes a legal entity as a subject of administrative responsibility within the framework of the mechanism of automatic recording of offences.

A special feature of administrative proceedings in cases of offences recorded in automatic mode is the issuance of a decision without drawing up a protocol and without direct participation in the implementation of administrative proceedings in accordance with articles 14-2, 258, 279-1 of the CUAO[4]. In the context of implementing the provisions of Article 14-2 of the CUAO, the legislator established a special mechanism for releasing the responsible person from administrative responsibility. This approach is aimed at ensuring a balance between the effectiveness of automated control and the principle of personalisation of legal responsibility, which is actively justified in contemporary administrative and legal doctrine. The normative model provides that exemption from liability is possible if actions defined by law are performed within twenty calendar days from the date of committing an offence or from the date of entry into force of the resolution. The basis for exemption from liability is documentary confirmation that the vehicle left the possession of a person as a result of illegal actions of third parties at the time of the offence. In addition, dismissal is possible in the case of a personal application of the actual driver with a plea of guilt and providing evidence of payment of the fine.

As a result of the study of the features of evidence, it was established that the main body of evidence in such cases is established using technical means of control (photo and video recordings, instrument metadata, register data), which makes it necessary to comply with increased standards of proof and ensure proper procedural guarantees for persons brought to administrative responsibility. In proceedings to challenge a decision, the person is required to rebut the facts and conclusions on which the decision of the public authority is based; this determines the specific nature of the exercise of the right to adduce evidence in such cases, as compared with the conventional model of administrative proceedings.

The procedural algorithm for executing the resolution provides for the transition to the stage of official notification of the responsible person by sending a registered letter, if the offender has not exercised the right to pay 50% of the fine within the preferential ten-day period established by law (according to Article 300-1 of the CUAO)[5]. This procedure not only ensures that the principle of the inevitability of legal liability is upheld, but also guarantees that the individual is properly informed of the penalties imposed on them, which is of critical importance for the observance of the procedural rights of road users.

Notification of the possibility to pay the fine is provided by supplying information on available official payment methods, including the use of a QR code placed on the front side of the decision, electronic services of the official website of the Ministry of Internal Affairs of Ukraine, the Driver's e-Cabinet, the "Diia" mobile application, and other payment systems and banking institutions operating legally within the territory of Ukraine.

The current legislation provides for the possibility of appealing a decision on the imposition of an administrative penalty in court or to a higher body (in accordance with articles 287-289 of the CUAO[6]) within the time period specified by law. An appeal is made by filing a complaint indicating the circumstances that refute the existence of elements of an administrative offence or prove the existence of grounds for exemption from liability.

From the standpoint of the principle of proportionality, the model of administrative responsibility for offences recorded in automatic mode requires an assessment through the prism of the balance between the public

[1] DSTU 8809:2018 Metrology "Traffic Rules Compliance Monitoring Devices with Photo and Video Recording Functions. Remote Vehicle Speed Meters and Remote Spatial and Temporal Vehicle Positioning Parameter Meters. Metrological and Technical Requirements". (2018, October). Retrieved from https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/dstu_8809-2018.pdf.
[2] Law of Ukraine No. 1314-VII "On Metrology and Metrological Activity". (2014, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1314-18.
[3] Code of Ukraine on Administrative Offences. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[4] Ibidem, 1984.
[5] Ibidem, 1984.
[6] Ibidem, 1984.

interest in ensuring road safety, and the rights of the person against whom the decision is made. In the case-law of the European Court of Human Rights, the proportionality of interference is traditionally assessed through the legitimacy of the aim pursued, the necessity of the measure applied, and the proportionality of the interference to the aim pursued. In the context of automatic recording, the legitimate goal is to ensure road safety, reduce accidents, and inevitably respond to traffic violations.

An analysis of the provisions of the CUAO shows that the legislator has provided for a special liability model that combines a simplified response procedure with subsequent procedural guarantees for a person. On the one hand, the person responsible for an offence recorded in automatic mode is the person defined by Article 14-2 of the CUAO, and a decision on such cases can be made without drawing up a protocol and without the direct participation of the person at the initial stage of proceedings in accordance with articles 258, 279-1-279-3 of the CUAO[1]. On the other hand, the CUAO provides for mechanisms that allow balancing the automated nature of recording: the ability to determine the proper user of the vehicle, the release of the responsible person from administrative responsibility in cases provided for by law, the appeal of the actual driver with an application for recognition of an offence, and the right to appeal the decision in court or to a higher authority.

This approach is consistent with the logic of the practice of the European Court of Human Rights, in particular in the cases of "Falk v. the Netherlands"[2] "O'halloran and Francis v. the United Kingdom"[3], where, in the field of road traffic, the use of specific models of liability is permitted, provided that individuals retain a genuine opportunity to protect their rights. Consequently, the proportionality of the Ukrainian model is ensured not only by the legitimate purpose of automated control, but also by the availability of procedural guarantees that allow verifying the validity of bringing to administrative responsibility, refute the presumption of liability or prove the existence of grounds for exemption from it.

In many countries, the system for the automatic detection of road traffic offences is regarded not only as a means of identifying individual offences, but also as part of a broader government policy on road safety. Its effectiveness is ensured by a combination of proper regulatory regulation, technical reliability of control tools, certainty of procedures for using the obtained data, and clear mechanisms for bringing to justice. In contrast, in Ukraine, the automatic recording system now functions mainly as an administrative-tort tool, focused primarily on detecting an offence and imposing an administrative penalty, and is aimed at strengthening control over road safety, compliance with traffic rules by its participants, preventing death and injury to people on the road network.

Practical interest for Ukraine is the experience of France, Great Britain and individual states of Australia, where certain elements of the functioning of automatic recording systems, in particular, statistical monitoring, technical approval of control tools, and evidence-based use of the obtained data, have a more detailed regulatory and organisational design. Thus, in France, the automated control system operates at the national level: as of January 1, 2024, it included 3,573 stationary or mobile radars, and 225 mobile radars operated by the police or on an outsourced basis; moreover, offences recorded by automatic cameras accounted for 78.1% of all road offences and 96.1% of all speed violations (ONISR, 2024). Compared to Ukraine, this model indicates not only a larger scale of use of automated control, but also a different level of statistical representation of its results in the road traffic enforcement system. In Ukraine, as of June 2026, there were 376 stationary technical means (monitoring devices) that record exceeding the established speed limits of vehicles, and violations of traffic rules and stopping on lanes for route vehicles. It should be borne in mind, however, that the development and expansion of the automated enforcement network in Ukraine are taking place against the backdrop of the Russian Federation's full-scale armed aggression against Ukraine, which began on 24 February 2022, and the associated security, financial, and organisational constraints. These indicators suggest a much larger scale of deployment of technical means in France, and the availability of detailed public statistics that allow assessing the actual role of automated control in the structure of road traffic enforcement system (Patrol Police Department of Ukraine, 2026).

In the UK, the use of automatic recording equipment for law enforcement purposes is allowed, provided that they pass the type approval procedure and meet the established technical requirements (GOV.UK, 2025). Compared to the Ukrainian model, the difference lies not in the fact that there are no technical requirements for such tools in Ukraine, but in a different design of their regulatory confirmation. In Ukraine, the legality of the use of technical means is ensured through the requirements of the technical regulations of legally regulated measuring equipment, DSTU 8809:2018[4], conformity assessment,

[1] Code of Ukraine on Administrative Offences. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[2] Judgment of the European Court of Human Rights in the Case No. 66273/01 "Falk v. the Netherlands". (2004, October). Retrieved from https://hudoc.echr.coe.int/eng?i=001-67305.
[3] Judgement of the European Court of Human Rights in the Case Nos. 15809/02 and 25624/02 "O'Halloran and Francis v. the United Kingdom". (2007, June). Retrieved from https://hudoc.echr.coe.int/eng?i=001-81359.
[4] DSTU 8809:2018 Metrology "Traffic Rules Compliance Monitoring Devices with Photo and Video Recording Functions. Remote Vehicle Speed Meters and Remote Spatial and Temporal Vehicle Positioning Parameter Meters. Metrological and Technical Requirements". (2018, October). Retrieved from https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/dstu_8809-2018.pdf.

and metrological verification procedures. That is, the Ukrainian model focuses primarily on the metrological suitability of measuring equipment. But the British type approval procedure has a special law enforcement purpose, since it is aimed at preliminary confirmation of the possibility of using a specific type of technical tool specifically for recording violations and gathering evidence. In this aspect, the British approach has a more pronounced special law enforcement purpose.

In the Australian states of New South Wales and Victoria, automated control is used as a component of road safety policy; in Victoria, photos and other data obtained by certified road cameras can be used as evidence of violations of the speed limit or driving at a red traffic light signal, while in New South Wales, automated cameras are used to detect and record such offences within the framework of the road enforcement system (Department of Justice and Community Safety, n.d.). Compared to Ukraine, this difference is not absolute, since Article 122 of the CUAO[1] provides for administrative liability for exceeding the established speed limits, driving on the forbidding traffic regulation signal, and other violations of traffic rules, and in case of their recording in automatic mode, the subject of liability is the responsible person defined in Article 14-2 of the CUAO. Thus, in terms of the range of offences, the Ukrainian model is comparable to the Australian approaches, since it also covers speed violations and some other traffic violations. The difference lies in the method of regulatory emphasis: in Ukraine, the relevant elements of offences and a special model of the responsible person are consolidated directly in the CUAO, while in the Australian jurisdictions more attention is paid to the relationship between the certified status of a traffic camera, automatically obtained data, and their evidentiary use in the framework of road traffic enforcement system.

Of additional interest is the Swedish approach, in which speed cameras are mostly placed not in isolation, but in series along a specific road section. This model allows assessing not only the point effect of the camera at the location of its installation, but also the change in driver behaviour between cameras and in the entire controlled area (Vadeby & Howard, 2024). Research findings indicate that, with this system of automated enforcement in place, a reduction in average speed is observed both in the immediate vicinity of the cameras and between them, which suggests that automated recording can be regarded as a tool for influencing the behaviour of road users.

The issue of personal data protection is of particular importance in this context, since the functioning of automatic recording systems involves the collection, processing and storage of visual information about vehicles, their registration numbers, place, time, and other circumstances of the recorded event. In New Zealand, when safety camera systems were introduced, these issues were the subject of a separate Privacy Impact Assessment, which assessed the legitimate purpose of data collection, the scope of access to the information, the retention periods and the risks to privacy. In Ukraine, the relevant issues are regulated by the general provisions of the legislation on personal data protection, and regulations defining the procedure for the functioning of the automatic recording system and the unified information system of the Ministry of Internal Affairs. The special regulation of automatic recording does not include a separate tool for preliminary assessment of the impact of such a system on privacy, comparable to the Privacy Impact Assessment (New Zealand Transport Agency, 2024). Therefore, the appropriate area for further development of the Ukrainian model is not to state the inconsistency of the current legislation with the principles of personal data protection, but to detail special guarantees of access to the received data, their storage periods, intended use, and control over the processing of information within the procedure defined by law.

Thus, the comparative analysis does not give grounds to assert that there is no regulatory framework for automatic recording in Ukraine. On the contrary, the Ukrainian model has its own regulatory structure, which includes the definition of a responsible person, special elements of administrative offences, the procedure for functioning of the system, registration of materials, implementation of the resolution and its appeal. The comparison with France, the United Kingdom, individual Australian states, Sweden, and New Zealand shows, however, that the potential for the further development of the Ukrainian system lies not so much in adopting international models as in refining specific elements of national regulation: a systematic statistical assessment of the effectiveness of automatic recording; specialised verification of the technical suitability of surveillance equipment for law enforcement purposes; a clear regulatory link between the certification of technical equipment, automatically collected data and its evidential value; an assessment of the behavioural impact of cameras on accident-prone sections of road; and the strengthening of specific safeguards for the protection of personal data.

An analysis of the Ukrainian model and selected international approaches provides grounds for proposing the authors' own typology of models for the use of automatically recorded data in the field of road safety (Table 1). The criterion for distinguishing such models is the legal and managerial significance of the information received: for establishing the fact of a separate offense, proving, statistical monitoring, evaluating the behaviour of drivers on a road section, protecting privacy, or responding to systematic violations.

[1] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.

Table 1. Author's typology of models for the use of automatically recorded data in the field of road safety

Model for using automatically recorded data	Model content	Country	Significance for the Ukrainian model
Recording-tort model	Data obtained automatically is used primarily to establish the fact of a specific administrative offence and to impose an administrative penalty.	Ukraine	Provides prompt response to traffic violations, but requires further clarification of the relationship between technical data, the responsible person, evidence, and procedural guarantees.
Technical and law enforcement model	Of paramount importance to confirm in advance that the technical device is suitable specifically for law enforcement purposes and for the generation of legally relevant data.	United Kingdom	Useful for detailing the Ukrainian approach in terms of specialised confirmation of the suitability of devices not only as measuring instruments, but as a source of evidence-based information.
Evidence-based certification model	Emphasis is placed on the relationship between the certified status of the traffic camera, automatically received photos, videos, and other data; the possibility of using them as evidence of a violation.	Victoria and New South Wales, Australia	Helps to strengthen the regulatory link between the certification of technical equipment, the reliability of the data obtained and their admissibility in administrative offence proceedings.
Statistical and management model	Automatic recording data is used not only for bringing to justice, but also for public assessment of the scale of offences, the effectiveness of cameras, and the role of automated control in the road safety system.	France	Allows moving from accounting for the number of cameras and resolutions to assessing the real impact of automatic recording on accidents, repetition of violations, and driver discipline.
Behavioural-plot model	Automatic recording is evaluated not only at the point where the camera is placed, but also by its impact on the behaviour of drivers on the entire road section, in particular between cameras.	Sweden	Gives grounds to evaluate the effectiveness of the system not only by the number of decisions issued, but also by changes in the speed behaviour of drivers in emergency areas.
Combined security model	Automatic locking is combined with other road safety measures, in particular with changing the speed limit, which enhances the overall preventive effect.		Shows that automatic recording can be more effective not as an isolated control tool, but as part of a comprehensive accident reduction policy.
Private guarantee model	Automatic recording is evaluated from the standpoint of personal data protection, access limits to information, storage periods, intended use, and privacy risks.	New Zealand	Useful for introducing special guarantees for data processing in the automatic recording system and the possible use of tools for preliminary assessment of the impact on privacy.
Risk-based model	Automatically recorded data can be used to assess not only a single violation, but also the repeatability, severity, and danger of driver behaviour.	Promising area for Ukraine	Enables a shift from a one-off fine system to a differentiated state response to systematic breaches of the Highway Code.

Source: compiled by the authors

The proposed typology allows considering automatic recording not as an isolated technical tool, but as an information and legal mechanism within which the same automatically obtained data can perform various functions: tort, evidence, management, behavioural, preventive, guarantee-related, and risk-oriented. For Ukraine, this means that the further development of the system must involve not only an increase in the number of technical monitoring devices, but also the establishment of a regulatory framework governing the legal status of data obtained through automatic recording.

Discussion

The results obtained give grounds to consider the system of automatic recording of traffic violations not only as a technical tool for detecting administrative offences, but as a comprehensive regulatory, procedural, and organisationally mediated mechanism of state influence on the behaviour of road users. This conclusion is generally consistent with the approach of A. Alobaidallah *et al*. (2025), which in a systematic review prove that the effectiveness of automated traffic enforcement systems depends not only on the technical characteristics of cameras, but also on the legal context of their implementation, the stability of law enforcement, and public perception of the relevant systems. The conducted research confirms this conclusion on the material of the Ukrainian model, since it shows that the legal significance of automatic recording does not arise at the time of technical detection of a violation as such, but within the framework of administrative proceedings, where the status of the responsible person, the permissibility of automatically obtained data, the procedure for issuing a decision, mechanisms for exemption from liability, and the possibility of appeal are important.

Conclusions of K. Shaaban *et al*. (2023), A. Vadeby & C. Howard (2024) and Z. Cheng *et al*. (2025) regarding the positive impact of automated control on reducing speed, improving driver discipline, and reducing accidents are important for substantiating the preventive function of such systems. The results of this study do not refute this approach, but allow considering it in a different plane. For the Ukrainian model, it is important not only to confirm the security effect of automatic recording, but also to show under what legal conditions such an effect can be achieved without disproportionately restricting individual rights. That is why this study focuses not only on the effectiveness of technical control, but also on procedural guarantees: determining the responsible person, the possibility of entering information about the proper user, the mechanism of exemption from liability and the right to appeal the decision.

Simultaneously, the results of J. Skubic *et al*. (2013) and E. De Pauw *et al*. (2014) show that the impact of automatic control cameras is not always uniform and may depend on the installation location, road context,

traffic intensity, and performance assessment methodology. These conclusions are a significant caveat for the Ukrainian model, since they do not allow automatically identifying an increase in the number of technical means with a guaranteed reduction in accidents. The analysis confirmed that, in order to assess the effectiveness of automatic enforcement in Ukraine, it is not sufficient to rely solely on statistics regarding the number of devices installed or the number of fines issued. A systematic assessment of the impact of cameras on accidents, driver behaviour, repetition of violations, and the level of appeal of decisions is necessary. In this aspect, international empirical research allows clarifying the area of further development of the Ukrainian system: it requires not only technical expansion, but also a publicly available analytical assessment of the results of functioning.

In this context, the study by A. Stagoff-Belfort *et al.* (2025) is particularly noteworthy; using data from New York, it analysed the impact of automatic speed enforcement cameras on road safety using a quasi-experimental approach. The significance of this study for the Ukrainian model is not only to confirm the potential safety effect of cameras, but also to demonstrate the need for a methodologically sound assessment of the results of their functioning. For Ukraine, this means that further expansion of the automatic recording system should be accompanied not only by an increase in the number of technical means, but also by regular analysis of their impact on accidents, the number of recorded violations, injuries, spatial concentration of accidents, and driver behaviour after the introduction of automatic control.

The study by N. Tilahun (2023), based on data on the operation of automatic speed cameras in Chicago, is of similar significance. The researcher, using the empirical Bayes approach, established a reduction in the number of road accidents resulting in fatalities and injuries in camera locations, in particular, a 12% reduction in fatal and injury crashes and a 15% reduction in fatality and severe injury crashes. Simultaneously, the study noted that not all controlled areas showed the expected safety effect. For the Ukrainian model, this conclusion is important, since it confirms the need to evaluate automatic recording not only on the fact of installing technical means, but also on the real results of their impact on the accident rate and severity of the consequences of road accidents in specific locations.

Also relevant is the study by E. Guerra *et al*. (2024), dedicated to evaluating the effectiveness of speed cameras at Roosevelt Boulevard in Philadelphia. The researchers, using Bayesian negative binomial and Poisson models, analysed the impact of cameras on the number of road accidents, injuries, and deaths on a dangerous urban highway and surrounding areas. The results of the study showed a decrease in accidents, injuries, and deaths after installing cameras compared to the control road segments. For the Ukrainian model, this source is important, as it confirms the feasibility of evaluating automatic recording not only as a national control tool, but also at the level of specific emergency areas where the placement of technical means should be justified by actual indicators of road danger.

A. Delbosc *et al*. (2025) complemented these findings, linking the effectiveness of automated speed enforcement with public perception of the fairness, transparency, and security of such programmes. For the Ukrainian context, this is of particular importance, since the automatic issuance of a decision without drawing up a protocol and without the direct participation of a person at the initial stage of proceedings can be perceived as an overly formalised model of responsibility. However, the analysis showed that such a model is not a purely automatic imposition of penalties, since the CUAO provides for a number of compensatory guarantees. The existence of these guarantees is a prerequisite for the legitimacy of the system and may influence the level of trust in the results of automatic recording.

In this regard, the position of O.P. Svitlychnyi (2023), who, in analysing traffic offences recorded by automated systems, drew attention to the duty of an authorised police officer to ascertain the circumstances of the offence based on factual evidence as defined by law, rather than placing the entire burden of proving innocence on the vehicle owner. The conducted research confirmed that the definition of a responsible person is the central element of the Ukrainian model, since it is through it that the legislator solves the problem of the impossibility of directly identifying the actual driver at the time of automatic recording. The findings give grounds to develop an appropriate approach: the problem is not only in determining the subject of responsibility, but also in ensuring an appropriate link between technical data, registration information, the presumption of responsibility, and the subsequent ability of a person to refute such a presumption.

Conclusions of O.V. Bytiak (2022) regarding the automatic recording of breaches of the Highway Code as a legal basis for initiating proceedings in cases of administrative offences are consistent with the results of this study. The author substantiated that the basis for initiating such a case is not the fact of recording the event using a technical means, but the receipt by an authorised police officer of an information file and metadata containing sufficient data about the event of an administrative offence. The provisions of the procedure for functioning of the system for recording administrative offences in the field of road safety in automatic mode, approved by resolution of the Cabinet of Ministers of Ukraine No. 833 of November 10, 2017[1], allowed

[1] Resolution of the Cabinet of Ministers of Ukraine No. 833 "On Approval of the Procedure for the Functioning of the System for Recording Administrative Offences in the Field of Road Safety in Automatic Mode". (2017, November). Retrieved from https://zakon.rada.gov.ua/laws/show/833-2017-%D0%BF.

considering the technical and informational components of such a system not only as organisational, but also as procedurally significant. The technical suitability of the device, the correctness of the software, the safety of automatically received data, and the procedure for accessing them are of direct importance for proof in an administrative offence case. Therefore, further improvement of the national model should concern not only the modernisation of technical infrastructure, but also the detailing of the rules for using automatically received information in proceedings.

Special attention should be paid to the conclusions of C. Slobogin & S. Brayne (2023), who examined state surveillance technologies through the prism of constitutional restrictions, the legality of data use, and privacy protection. The conducted study confirmed the relevance of this approach for systems for automatic recording of traffic violations. Although the Ukrainian system has a legitimate security purpose, its functioning is related to the collection and processing of data on vehicles, the place, time, and circumstances of a recorded event. Therefore, the issue of privacy cannot be considered as a secondary one. Unlike broader models of digital surveillance, automatic recording of road offences has a narrower functional purpose, which makes it possible to justify its permissibility, provided that the boundaries of information collection, storage, access, and use are clearly defined.

Thus, the results of the study are generally consistent with contemporary scientific approaches, according to which automated control in the field of road traffic should be evaluated simultaneously according to the criteria of efficiency, legal certainty, technical reliability, and respect for human rights. The analysis allows clarifying these approaches in relation to the Ukrainian context. For Ukraine, the key is not only the further expansion of the network of technical means, but also the detailing of the relationship between the technical suitability of devices, the evidential value of automatically obtained data, procedural guarantees of the person, and the protection of personal information. This is the main contribution of the study to the development of administrative and legal understanding of the system of automatic recording of offences in the field of road safety.

Conclusions

The subject of the study was the system of recording administrative offences in the field of road safety in automatic mode, in particular, the features of its regulatory consolidation, organisation, and application in Ukraine in comparison with individual international models. This purpose was achieved because the study analysed the regulatory framework for the functioning of this system, established its procedural features, examined individual international approaches, and clarified their significance for understanding the national model.

It was revealed that the Ukrainian model of automatic recording has its own regulatory structure, which combines the provisions of administrative and tort legislation, by-law regulation of the system's functioning, technical and metrological requirements for controls, and a special procedure for administrative proceedings. The analysis of the legislation helped to establish that the key elements of this model are the determination of the responsible person, the issuance of a decision without drawing up a protocol and without the direct participation of the person at the initial stage of proceedings, the possibility of exemption from liability, the implementation of the decision, and its appeal. The results of the study showed that the evidence base in cases of this category is formed mainly due to technical means of control, photo and video data, metadata of devices, and information from registers, which leads to an increased importance of the technical suitability of means of recording and procedural guarantees of a person. Comparative analysis showed that foreign approaches are valuable not as ready-made models for direct borrowing, but as a source of separate functional benchmarks: statistical performance monitoring, specialised technical approval, evidence-based use of data from certified cameras, assessment of the behavioural impact of cameras on road sections, and preliminary assessment of privacy risks.

Summarising the results obtained, it can be noted that automatic recording should not be considered only as a technical method for detecting violations or as a simplified mechanism for imposing a fine. Conceptually, it appears as information and legal mechanism within which automatically obtained data can perform tort, evidence, management, behavioural, preventive, guarantee, and risk-oriented functions. It is this approach that deepens the understanding of the Ukrainian model, as it shifts the focus from the number of technical means and regulations to the legal regime of data, their evidentiary quality, connection with procedural guarantees, and importance for road safety.

Promising areas for further research include the analysis of case law relating to appeals against decisions, an examination of the standards governing the use of technically obtained data as evidence, and an investigation into mechanisms for striking a balance between the public interest in road safety, and an person's right to due process.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Alobaidallah, A.M., Alqahtani, A., & Maniruzzaman, H.M. (2025). Safety effectiveness of automated traffic enforcement systems: A critical analysis of existing challenges and solutions. *Future Transportation*, 5(1), article number 25. doi: 10.3390/futuretransp5010025.

[2] Amancio, E.C., Gadda, T.M.C., Corrêa, J.N., Bonetti, G.D.C., Oviedo-Trespalacios, O., & Bastos, J.T. (2024). Impact of speed limit enforcement cameras on speed behavior: Naturalistic evidence from Brazil. *Transportation Research Record*, 2678(9), 807-822. doi: 10.1177/03611981241230548.

[3] Bytiak, O.V. (2022). Automatic recording of traffic rules violations as a legal ground for initiating proceedings in an administrative offense case. *Legal Scientific Electronic Journal*, 8, 240-243. doi: 10.32782/2524-0374/2022-8/50.

[4] Cheng, Z., Dong, Z., & Pang, M.-S. (2025). Automated enforcement and traffic safety. *Management Science*, 71(12), 10067-10087. doi: 10.1287/mnsc.2023.00575.

[5] De Pauw, E., Daniels, S., Brijs, T., Hermans, E., & Wets, G. (2014). An evaluation of the traffic safety effect of fixed speed cameras. *Safety Science*, 62, 168-174. doi: 10.1016/j.ssci.2013.07.028.

[6] Delavary, M., Mesic, A., Krebs, E., Sesonga, P., Uwase-Gakwaya, B., Nzeyimana, I., & Vanlaar, W. (2024). Assessing the effect of automated speed enforcement and comprehensive measures on road safety in Rwanda. *Traffic Injury Prevention*, 25(7), 947-955. doi: 10.1080/15389588.2024.2354901.

[7] Delbosc, A., Muir, C., Ralph, K., Barajas, J. M., & Johnson-Rodriguez, A. (2025). Do perceptions of speeding act as a barrier to automated speed enforcement in the United States? *Transportation Research. Part F: Psychology and Behaviour*, 114, 1042-1052. doi: 10.1016/j.trf.2025.07.010.

[8] Department of Justice and Community Safety. (n.d.). *Evidence of infringement captured by road safety cameras*. Retrieved from https://www.vic.gov.au/evidence-infringement.

[9] Gao, J., Yang, D., Xu, C., Ozbay, K., & Sharma, S. (2025). Assessing the impact of fixed speed cameras on speeding behavior and crashes: A longitudinal study in New York City. *Transportation Research Interdisciplinary Perspectives*, 30, article number 101373. doi: 10.1016/j.trip.2025.101373.

[10] GOV.UK. (2025). *Speedmeter, traffic light and prohibited lane enforcement camera handbook*. Retrieved from https://www.gov.uk/government/publications/speedmeter-traffic-light-and-lane-enforcement-camera-handbook/speedmeter-traffic-light-and-prohibited-lane-enforcement-camera-handbook-accessible.

[11] Guerra, E., Puchalsky, C., Kovalova, N., Hu, Y., Si, Q., Tan, J., & Zhao, G. (2024). Evaluating the effectiveness of speed cameras on Philadelphia's Roosevelt Boulevard. *Transportation Research Record: Journal of the Transportation Research Boa*rd, 2678(9), 452-461. doi: 10.1177/03611981241230320.

[12] Howard, A.W., Batomen, B., Zubair, S., Cloutier, M.-S., Macpherson, A.K., & Rothman, L. (2025). Automated speed enforcement reduced vehicle speeds in school zones in Toronto: A prospective quasi-experimental study. *Injury Prevention*. doi: 10.1136/ip-2024-045561.

[13] Ivanovska, M., Kreft, J., Štruc, V., & Perš, J. (2025). Privacy-by-design AIoT vision for intelligent urban environments. *Journal of Systems Architecture*, 169, article number 103586. doi: 10.1016/j.sysarc.2025.103586.

[14] Luca, C. (2024). *The impact of automated enforcement systems on traffic management efficiency*. Retrieved from https://surl.li/pmhwmt.

[15] New York City Department of Transportation. (2024). *New York City automated speed enforcement program: 2024 report*. Retrieved from https://www.nyc.gov/html/dot/downloads/pdf/speed-camera-report.pdf.

[16] New Zealand Transport Agency. (2024). *Safety camera privacy impact assessment*. Retrieved from https://www.nzta.govt.nz/assets/Safety/docs/safety-cameras/safety-camera-privacy-impact-assessment.pdf.

[17] Observatoire National Interministeriel de la Securite Routiere (ONISR). (2024). *2023 road traffic violations annual report*. Retrieved from https://www.onisr.securite-routiere.gouv.fr/en/road-safety-performance/annual-reports-offences-and-demerit-points/2023-road-traffic-violations-annual-report.

[18] Patrol Police Department of Ukraine. (2026). *6 years of the automated traffic violation recording system. Patrol Police of Ukraine*. Retrieved from https://surl.li/jafqjy.

[19] Safavi-Naini, S.A.A., *et al*. (2024). Drivers' behavior confronting fixed and point-to-point speed enforcement camera: Agent-based simulation and translation to crash relative risk change. *Scientific Reports*, 14, article number 1863. doi: 10.1038/s41598-024-52265-3.

[20] Sebapalo, M., Morobe, P., Kekgathetse, M.B., Gobonamang, T.K., & Motshidisi, K. (2025). Evaluating the role of traffic surveillance cameras in enhancing road safety in Greater Gaborone. *International Journal of Development and Sustainability*, 14(9), 647-663. doi: 10.63212/IJDS25040103.

[21] Shaaban, K., Mohammad, A., & Eleimat, A. (2023). Effectiveness of a fixed speed camera traffic enforcement system in a developing country. *Ain Shams Engineering Journal*, 14, article number 102154. doi: 10.1016/j.asej.2023.102154.

[22] Skubic, J., Johnson, S.B., Salvino, C., Vanhoy, S., & Hu, C. (2013). Do speed cameras reduce collisions? *Journal of Transportation Safety & Security*, 5(3), 214-230.
[23] Slobogin, C., & Brayne, S. (2023). Surveillance technologies and constitutional law. *Annual Review of Criminology*, 6, 219-240. doi: 10.1146/annurev-criminol-030421-035102.
[24] Stagoff-Belfort, A., Ben-Menachem, J., & Beck, B. (2025). Can speed cameras make streets safer? Quasi-experimental evidence from New York City. *Proceedings of the National Academy of Sciences*, 122(50), article number e2520328122. doi: 10.1073/pnas.2520328122.
[25] Svitlychnyi, O.P. (2023). Violations of traffic rules recorded in automatic mode: Selected issues. *Scientific Bulletin of Public and Private Law*, 3, 103-107. doi: 10.32844/2618-1258.2023.3.17.
[26] Tilahun, N. (2023). Safety impact of automated speed camera enforcement: Empirical findings based on Chicago's speed cameras. *Transportation Research Record: Journal of the Transportation Research Board*, 2677(1), 1490-1498. doi: 10.1177/03611981221104808.
[27] Vadeby, A., & Howard, C. (2024). Spot speed cameras in a series: Effects on speed and traffic safety. *Accident Analysis & Prevention*, 199, article number 107525. doi: 10.1016/j.aap.2024.107525.
[28] Valderrama, S. L., Santana Palacios, M., Perdomo Botello, V., Perez-Barbosa, D., Vega Arrieta, J., Kisner, J., & Adriazola-Steil, C. (2024). On speed management, public health, and risky behaviors: Examining the side effects of automated speed-enforcement cameras on traffic crashes in Bogotá, Colombia. *Transportation Research Record*, 2678(3), 590-600. doi: 10.1177/03611981231182419.

Система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі

Ольга Марків
Головний інспектор
Департамент патрульної поліції Національної поліції України
03048, вул. Федора Ернста, 3, м. Київ, Україна
https://orcid.org/0009-0005-6453-7389

Ольга Бичкова
Інспектор
Головне управління Національної поліції в Одеській області
65014, вул. Єврейська, 12, м. Одеса, Україна
https://orcid.org/0009-0008-7590-4721

Євгенія Мурзо
Доктор філософії в галузі права, старший слідчий
Головне слідче управління Національної поліції України
01024, вул. Академіка Богомольця, 10, м. Київ, Україна
https://orcid.org/0009-0000-4409-0560

Анотація
Актуальність дослідження зумовлена впровадженням систем автоматичної фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху та необхідністю їх належного нормативного, організаційного і процесуального переосмислення в умовах цифровізації державного контролю. Метою статті було дослідження особливостей нормативного закріплення, організації та застосування системи автоматичної фіксації порушень Правил дорожнього руху в Україні та окремих державах. У роботі використано формально-юридичний, системно-структурний, порівняльно-правовий, логіко-семантичний та аналітичний методи. За результатами дослідження встановлено, що нормативно-правову основу функціонування системи автоматичної фіксації в Україні формують положення кодифікованого адміністративного законодавства, підзаконні акти уряду й акти відомчого регулювання, які в сукупності визначають матеріально-правові, організаційно-технічні та процедурні засади її роботи. Виявлено, що українська модель вирізняється спеціальним визначенням відповідальної особи, винесенням постанови без складання протоколу та без безпосередньої участі особи під час здійснення адміністративного провадження. Доведено, що доказова база у справах цієї категорії формується технічними засобами контролю і даними реєстрів, що зумовлює специфічний характер процесуальних гарантій. З'ясовано, що стадія виконання постанови має самостійне значення для забезпечення належного інформування особи та реалізації процесуальних прав. Порівняльний аналіз засвідчив, що у Франції, Великій Британії, окремих штатах Австралії та Новій Зеландії автоматична фіксація поєднується з розвиненими механізмами технічного схвалення засобів контролю, використанням автоматично отриманих даних як доказів. Дослідження має практичне значення для подальшого розвитку національної моделі в частині правової визначеності, допустимості використання автоматично отриманих даних, технічної придатності засобів контролю та гарантування приватності учасників дорожнього руху

Ключові слова:
адміністративна відповідальність; відповідальна особа; автоматизований контроль швидкості; доказове значення технічних даних; оскарження постанови; захист персональних даних; порівняльно-правовий аналіз

UDC 342:346.546
DOI: 10.63341/naia-chasopis/2.2026.75

ISSN 2519-4216
E-ISSN 2519-4313

Constitutional and legal aspects of improving the mechanism for countering monopolism and unfair competition

Murad Orujov*
Master, PhD Student, Senior Contracts Specialist
National Aviation Academy
AZ1045, 30 Mardakan Ave., Baku, Azerbaijan
https://orcid.org/0009-0002-7169-8453

Abstract
The aim of the study was to identify areas for improving constitutional and legal mechanisms to countering monopolism and unfair competition. Formal-legal, comparative-legal, case-study, and legal modelling methods were used. The study demonstrated that the constitutional and legal model for regulating competition in the Republic of Azerbaijan is based on a combination of guarantees of freedom of entrepreneurship and the permissibility of state intervention to limit monopolistic activity. It was established that the previous antimonopoly regulation system, established between 1993 and 1998, was characterised by fragmented legal regulation, insufficient coordination of mechanisms for controlling economic concentration, dominant positions, and unfair competition, and was focused on suppressing existing violations. The study substantiated the need to improve legal mechanisms for preventing anticompetitive behaviour, strengthen controls over economic concentration, and adapt competition legislation to the conditions of the digital economy. A comparative-legal analysis of the current legislation of the Republic of Azerbaijan, European Union legislation, and international approaches to competition regulation demonstrated Azerbaijan's transition to a systemic model of competition control, which provides for the interrelated regulation of economic concentration, dominance, and unfair competition, as well as the partial implementation of international competition law standards. As a comparative context, it was established that international anti-monopoly mechanisms evolved from monitoring cartels and abuse of dominance to preventive regulation of digital markets and the platform economy. It was also revealed that the European Union developed a specific model for regulating digital platforms in 2020-2025, extending antimonopoly control to algorithmic governance, the use of user data, and digital infrastructure. The results of the study can be used by the legislature of the Republic of Azerbaijan, bodies implementing state competition policy and antimonopoly control, and academic institutions in improving competition legislation, developing mechanisms for regulating digital markets, and preparing proposals for harmonising the national antimonopoly control system with international competition law standards

Keywords:
economic concentration; dominant position; market power; digital platforms; international standards

Article's History:
Received: 03.02.2026
Revised: 01.05.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Orujov, M. (2026). Constitutional and legal aspects of improving the mechanism for countering monopolism and unfair competition. *Law Journal of the National Academy of Internal Affairs*, 16(2), 75-89. doi: 10.63341/naia-chasopis/2.2026.75.

*Corresponding author (*mrd.orujov@outlook.com*)

Introduction

The relevance of this study stems from the need to improve legal mechanisms for countering monopolism in the context of the digital transformation of the economy and the globalisation of economic relations. Despite the development of international and national competition legislation, current regulatory mechanisms remain insufficiently adapted to the cross-border nature of corporate activities, the proliferation of digital platforms, and new ways of restricting competition through the use of data and algorithmic technologies. Ensuring a balance between constitutional principles of freedom of economic activity and the permissible limits of government intervention in competitive relations is of additional scientific significance, requiring further research into international experience and the development of effective approaches to improving antitrust policy.

In the academic literature, issues of countering monopolism and unfair competition are considered in the context of the digital transformation of the economy, constitutional guarantees of economic freedom, and increased government regulation of markets. K. Abdullayev *et al.* (2024) found that the development of the digital economy in Azerbaijan is accompanied by the expansion of digital infrastructure, electronic services, and platform business models. The authors noted that the country is gradually strengthening its position in international digital development rankings; however, structural limitations to digital competitiveness persist. In particular, according to the data provided in the study, Azerbaijan ranked 87th in the Information and Communication Technologies Development Index, 83rd in the E-Government Development Index, and 75th in the Network Readiness Index, indicating a persistent gap with countries leading in digital transformation. Similar conclusions are presented in the study by T. Guluzade (2025), who links the prospects for Azerbaijan's digital development to the need for institutional strengthening of economic regulation mechanisms. The author demonstrated that the proliferation of digital platforms is accompanied by increasing economic dependence of industries such as e-commerce, digital advertising, online payments, and platform services on a limited number of major market participants, increasing the risk of market power concentration. The study also concludes that the insufficient adaptation of legal mechanisms to the conditions of digitalisation may contribute to a weakening of the competitive environment and limiting the economic freedom of business entities. The constitutional and legal aspects of competition policy are explored in the study by M. Bernatt (2025). The study demonstrates that the protection of competition is linked to the implementation of the principles of fairness, equality of economic opportunity, and public welfare. The researcher concluded that constitutional norms are used as a guide in determining the permissible limits of market concentration and state intervention in the economy.

The problem of transforming European competition policy in the context of digitalisation is examined by M. Cini & P. Czulno (2022). The authors found that the formation of the European Union's single digital market necessitated a revision of the traditional approach to competition regulation, as traditional antitrust mechanisms did not provide sufficient oversight of large digital platforms. The study found that European Union policy is gradually shifting from responding to existing violations to preventing potential risks to the competitive environment. This development is also reflected in the work of E. Fazio (2022), who focuses on the challenges of the digital transition for competition law. The author substantiated that existing legal framework insufficiently account for the specific functioning of digital platforms based on the use of big data and network effects. Among the study's findings, the need to develop new criteria for assessing dominant market position is noted, as traditional indicators of market power do not fully reflect the influence of digital entities on the competitive environment. R. Podszun (2023) examined the transition from traditional antitrust regulation to specialised mechanisms for monitoring digital platforms. The author concludes that the adoption of Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)"[1] signals the emergence of a separate regulatory regime for large digital intermediaries. The study establishes that the European regulatory model is focused on preventing abuses by the largest digital platforms even before formal violations of antitrust laws arise.

The importance of public policy in ensuring conditions for the development of competition is explored in the work of A. Guliyeva (2025). The researcher found that between 2020 and 2025, the Republic of Azerbaijan expanded support programmes for small and medium-sized enterprises, financial instruments for stimulating business, and digital services for business entities. The results indicate that state support for entrepreneurship contributed to improved market access and increased economic activity, but also highlighted the need to ensure equal competitive conditions for all market participants. The author concludes that the effectiveness of economic reforms depends not only on the scale of state support but also on the functioning of legal mechanisms for the protection of competition,

[1] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.

which can prevent excessive market concentration and the creation of unjustified advantages for certain economic entities. The study by O. Bakalinska *et al*. (2022) focuses on the role of the state in ensuring a competitive environment. The authors conclude that the protection of competition is acquiring the character of a comprehensive public-law function associated with ensuring the economic security of the state. The paper notes that countering monopolism cannot be limited to private law mechanisms, as a significant portion of anticompetitive practices are shaped by institutional and administrative factors. A. Khalilov (2024) further elucidates the constitutional foundations of state regulation in Azerbaijan through the author's study of the principle of subsidiarity. The author found that the distribution of powers among state institutions should ensure a balance between centralised control and the autonomy of economic entities. The researcher also substantiated that the principle of subsidiarity can be used as a mechanism to prevent excessive state intervention in competitive relations while maintaining the ability to respond to threats of market monopolisation.

Despite a significant number of studies devoted to the digital transformation of competition law, the regulation of platform markets, and the modernisation of competition legislation, the scientific literature remains insufficiently developed on the relationship between constitutional principles, state regulation mechanisms, and modern forms of countering monopolism in the digital economy. Limited attention is given to a comprehensive analysis of the integration of constitutional and legal guarantees of economic freedom with administrative and antitrust mechanisms for regulating digital markets.

The purpose of the study was to identify the constitutional and legal aspects of improving the system for countering monopolism and unfair competition. The objectives of the study were to: explore international approaches to countering monopolism and unfair competition in the context of economic digitalisation; analyse the constitutional and legal framework for regulating competition and restricting monopolistic activity in the Republic of Azerbaijan; identify existing gaps in legal regulation in this area; and identify areas for improving competition legislation.

Materials and Methods

The methodological design of the study was based on a combination of formal-legal, comparative-legal, and legal modelling methods. The Republic of Azerbaijan was chosen as the main object of the study due to the reform of national competition legislation, the adoption of the Competition Code of the Republic of Azerbaijan[1], and the adaptation of antimonopoly control mechanisms to international standards. The formal-legal method was used in the study. The regulatory framework for the study was based on the Constitution of the Republic of Azerbaijan[2], the Competition Code of the Republic of Azerbaijan[3], and the Law of the Republic of Azerbaijan No. 526 "On Anti-Monopoly Activities"[4]. The provisions of these acts were used to study the constitutional guarantees of freedom of entrepreneurship, the legal basis for protecting competition, the regulation of dominant positions, economic concentration, and restrictions on monopolistic activity. To study the features of the previously existing system of competition regulation, the provisions of Law of the Republic of Azerbaijan No. 1049 "On Unfair Competition"[5] and the Law of the Republic of Azerbaijan No. 590-IQ "On Natural Monopolies"[6] were used.

A comparative-legal method was used to compare the antimonopoly control system of the Republic of Azerbaijan with international approaches to competition regulation. In examining international standards for preventing anticompetitive agreements and restricting monopolistic activity, the Recommendation of the Council concerning effective action against hard core cartels (Organisation for Economic Co-operation and Development, 2025), the United Nations Set of Principles and Rules on Competition (United Nations Conference on Trade and Development, 2000), and the Consolidated version of the Treaty on the Functioning of the European Union[7] were used. To analyse the international legal principles of non-discrimination, equal access to markets, and ensuring fair conditions for economic activity, the provisions of the General Agreement on Tariffs and Trade (GATT 1947)[8], the General Agreement on Trade in Services (GATS)[9], and the Agreement on Trade-Related Aspects of Intellectual Property Rights

[1] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.
[2] Constitution of the Republic of Azerbaijan. (1995, November). Retrieved from https://president.az/en/pages/view/azerbaijan/constitution.
[3] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.
[4] Law of the Republic of Azerbaijan No. 526 "On Anti-Monopoly Activities". (1993, March). Retrieved from https://wipolex-res.wipo.int/edocs/lexdocs/laws/az/az/az025az.pdf?last-modified=1305040098&.
[5] Law of the Republic of Azerbaijan No. 1049 "On Unfair Competition". (1995, June). Retrieved from https://wipolex-res.wipo.int/edocs/lexdocs/laws/az/az/az125az_1.pdf?last-modified=1765787537&Expires=1782371184&Signature=pEvv8vBGlx~.
[6] Law of the Republic of Azerbaijan No. 590-IQ "On Natural Monopolies". (1998, December). Retrieved from http://binegedi-ih.gov.az/storage/files/files/15_12_1998%20-%20T%C9%99bii%20inhisarlar%20%20haqq%C4%B1nda%20Az%C9%99rbaycan%20Respublikas%C4%B1n%C4%B1n%20Qanunu.pdf.
[7] Consolidated version of the Treaty on the Functioning of the European Union. (2012, October). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.
[8] General Agreement on Tariffs and Trade (GATT 1947). (1947, October). Retrieved from https://www.wto.org/english/docs_e/legal_e/downloads_e/GATT1947_en.pdf.
[9] General Agreement on Trade in Services. (1994, April). Retrieved from https://jusmundi.com/en/document/treaty/en-general-agreement-on-trade-in-services-1994-general-agreement-on-trade-in-services-1994-friday-15th-april-1994.

(TRIPS)[1] were applied. A comparison of modern mechanisms for regulating digital markets was carried out on the basis of Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)"[2] and Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)"[3]. The comparison was carried out based on the criteria of regulating dominant positions, controlling economic concentration, preventing unfair competition, regulating digital platforms and applying preventive antimonopoly control mechanisms. The comparative-legal method was used to determine the extent of implementation of international competition law standards in the legislation of the Republic of Azerbaijan and to identify limitations in national regulation of digital markets.

The case-study method was used to examine decisions, investigations, and official communications of the European Commission regarding the digital platforms Google, Apple, Amazon, and Meta. Its application was aimed at identifying the specifics of the legal assessment of digital platforms' behaviour, define criteria for assessing market power, and identify trends in the development of competition regulation mechanisms for digital markets in the European Union. The analysis included official antitrust decisions and procedural documents of the European Commission related to investigations against Google (Antitrust: Commission fines…, 2019), Amazon (Antitrust: Commission sends…, 2020), Apple (Antitrust: Commission sends…, 2021), and Alphabet, Apple, and Meta under the Digital Markets Act (Directorate-General for Competition & Directorate-General for Communications Networks, Content and Technology, 2024). These documents were selected as representative examples of the practical application of European competition law to major digital platforms and made it possible to trace the evolution of the European Union's approaches to regulating market concentration and limiting anticompetitive behaviour in the digital economy. Legal modelling was used to develop proapective areas for improving the competition legislation of the Republic of Azerbaijan, including clarifying the criteria for determining a dominant position in digital markets, developing mechanisms for preliminary control of economic concentration, regulating the activities of digital platforms, and introducing specialised tools for assessing the risks of restricting competition in the digital sector.

Results

International approaches to countering monopolism and unfair competition. Competition law regulates social relations related to ensuring the functioning of a market economy, implementing the principle of free entrepreneurial activity, and limiting monopolistic activities of economic entities. International practice views the protection of competition as a prerequisite for maintaining stable economic relations, developing entrepreneurship, preventing the abuse of market power, and ensuring a balance between private and public interests. Thus, in European Union law, the prohibition on the abuse of a dominant position, enshrined in Article 102 of the Consolidated version of the Treaty on the Functioning of the European Union[4], aims to prevent situations in which large economic entities can restrict competitors' access to the market, impose unfair business conditions, or create obstacles to innovation. In most countries, countering monopolism is associated not only with the need to maintain economic efficiency but also with ensuring equality among market participants, protecting consumer rights, and limiting excessive concentration of economic power. The United Nations Conference on Trade and Development (2024) emphasises that excessive concentration of market power can lead to the formation of structural barriers to entry, limited access of economic entities to key resources and distribution channels, and increased economic dependence of small and medium-sized enterprises on large corporate groups. Such processes can reduce the intensity of competition and limit the development opportunities of new market entrants. Consequently, competition law gradually came to be used not only as an instrument of economic regulation, but also as a legal mechanism for ensuring a level playing field for economic activity.

The development of international approaches to countering monopolism was accompanied by changes in the content of antitrust regulation (Kovacic & Shapiro, 2000). Initially, international antitrust regulation focused on preventing cartels, price fixing, and abuse of dominant positions by large industrial associations. Subsequently, the development of transnational

[1] Agreement on Trade-Related Aspects of Intellectual Property Rights. (1994, April). Retrieved from https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[2] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.
[3] Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
[4] Consolidated version of the Treaty on the Functioning of the European Union. (2012, October). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.

corporations, the globalisation of markets, and the changing structure of economic relations led to an expansion of the scope of competition regulation. International practice expanded the scope of competition regulation to include mechanisms for monitoring economic concentration, assessing the impact of cross-border mergers and acquisitions, and taking into account the impact of digital platforms on the competitive environment. At the same time, the scope of antimonopoly control expanded to include issues of access to digital infrastructure, data use, and limiting the market power of entities with significant economic influence. As a result, competition law became comprehensive and includes both measures to prevent anticompetitive behaviour and preventive mechanisms for monitoring the market activities of economic entities. The development of international approaches to protecting competition was accompanied by the formation of a system of supranational competition policy standards developed by international organisations. The activities influenced the unification of antitrust regulation mechanisms, the development of fair competition principles, and the adaptation of national legislation to changes in the global economy (Table 1).

Table 1. International approaches to regulating competition and countering monopolism

International organisation	Main directions of competition policy	Mechanisms to countering monopolism	Approaches to preventing unfair competition	Significance for national legislation
Organisation for Economic Cooperation and Development	Development of recommendations for improving competition policy, ensuring market transparency and developing antimonopoly control mechanisms	Control of economic concentration, improvement of antitrust investigation procedures, development of mechanisms for preliminary assessment of market risks	Restricting anticompetitive agreements, preventing abuse of dominant positions, and regulating the activities of digital platforms	It is used by states when modernising competition legislation and reforming the antimonopoly control system
United Nations Conference on Trade and Development	Formation of approaches to ensuring a competitive environment as a condition for sustainable economic development	Support for mechanisms to limit market concentration and regulate the activities of transnational corporations	Preventing discriminatory market access conditions and protecting small and medium-sized businesses	It is used in the development of competition legislation in countries with developing and transforming economies
World Trade Organisation	Ensuring the principles of non-discriminatory international trade and equal access to markets	Formation of conditions for non-discriminatory access to markets that affect the competitive environment in international trade	Prevention of discriminatory trade practices and restrictions on access to foreign markets	Promotes the harmonisation of trade and competition laws of the participating states
European Union	Formation of a unified competition policy within the framework of a common market	Control of enterprise concentration, prevention of abuse of dominant position, antitrust investigations	Regulating the activities of digital platforms and limiting unfair practices in e-commerce	The European model is used in reforming national competition regulation systems

Source: compiled by the author based on United Nations Conference on Trade and Development (2000), Organisation for Economic Co-operation and Development (2025), Consolidated version of the Treaty on the Functioning of the European Union[1], General Agreement on Tariffs and Trade (GATT 1947)[2], General Agreement on Trade in Services[3], Agreement on Trade-Related Aspects of Intellectual Property Rights[4], Regulation (EU) No. 2022/1925 of the European Parliament and of the Council[5], Regulation (EU) No. 2022/2065 of the European Parliament and of the Council[6]

The general approaches of international organisations to protecting competition are based on the recognition of the need to limit excessive concentration of economic power and ensure a level playing field for economic activity. However, the regulatory mechanisms for implementing competition policy vary depending on the legal nature of the international organisation and its area of competence. Thus, the OECD's activities are aimed at developing recommendations and soft law standards used by states when reforming national competition legislation. In particular, the Recommendation of the Council concerning effective action against hard core cartels (Organisation for Economic Co-operation and Development, 2025) sets out approaches to suppressing

[1] Consolidated version of the Treaty on the Functioning of the European Union. (2012, October). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.
[2] General Agreement on Tariffs and Trade (GATT 1947). (1947, October). Retrieved from https://www.wto.org/english/docs_e/legal_e/downloads_e/GATT1947_en.pdf.
[3] General Agreement on Trade in Services. (1994, April). Retrieved from https://jusmundi.com/en/document/treaty/en-general-agreement-on-trade-in-services-1994-general-agreement-on-trade-in-services-1994-friday-15th-april-1994.
[4] Agreement on Trade-Related Aspects of Intellectual Property Rights. (1994, April). Retrieved from https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[5] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.
[6] Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

cartels, developing international cooperation between competition authorities, and improving procedures for investigating anticompetitive behaviour. Organisation for Economic Co-operation and Development (2024) documents substantiate the need to expand traditional antimonopoly control mechanisms by taking into account the network effects of digital platforms, the use of algorithmic pricing systems, and the concentration of data as a source of market power. Particular attention is paid to improving mechanisms for monitoring digital markets, increasing the transparency of algorithmic decisions, and developing tools for identifying anticompetitive practices in the digital environment.

The United Nations Conference on Trade and Development (2000) approach has a different legal focus and is associated with ensuring the balanced economic development of states. The provisions of the United Nations Set of Multilaterally Agreed Equitable Principles and Rules for the Control of Restrictive Business Practices, which stipulate the need to prevent the abuse of market power, limit anticompetitive agreements, and ensure fair conditions for economic entities' access to markets, are of significance for international practice. In contrast to the Recommendation of the Council concerning effective action against hard core cartels (Organisation for Economic Co-operation and Development, 2025), which is focused primarily on improving mechanisms for identifying and suppressing cartels, the provisions of the United Nations Set of Principles and Rules on Competition provide for a broader approach to competition regulation. The UNCTAD Set views competition law as a tool for creating conditions for the development of small and medium-sized businesses, preventing excessive economic concentration, expanding access for new entrants to markets, and reducing the dependence of the national economy on a limited number of large economic entities. The World Trade Organisation (WTO) regulatory approach is based on regulating international trade and ensuring non-discriminatory market access. While the WTO lacks a single, codified antitrust act, certain competition-related provisions are contained in the General Agreement on Tariffs and Trade[1], General Agreement on Trade in Services[2], and Agreement on Trade-Related Aspects of Intellectual Property Rights[3]. These instruments enshrine the principles of non-discrimination, transparency, and equal access to international trade, which influence the formation of a competitive environment in cross-border economic relations. As a result, competition policy within the WTO is implemented through limiting trade barriers and preventing practices that could create unfair advantages for certain international market participants.

The European Union developed a comprehensive system of competition regulation, which includes mechanisms for monitoring economic concentration, limiting abuse of dominance, and preventing anticompetitive agreements[4]. It is considered one of the most developed regional competition protection regimes. The legal basis for European Union competition policy is Articles 101-109 of the Consolidated version of the Treaty on the Functioning of the European Union, which prohibit anticompetitive agreements, abuse of a dominant position, and anticompetitive state aid. Unlike the advisory nature of OECD and UNCTAD acts, EU law is legally binding on Member States and is accompanied by a developed system of supranational oversight.

The development of the digital economy and increasing market concentration in digital services led to reforms of European competition law in 2020-2025. These changes were associated with the adoption of the Regulation (EU) No. 2022/1925 of the European Parliament and of the Council[5] and the Regulation (EU) No. 2022/2065 of the European Parliament and of the Council[6]. The adoption of these acts was the European Union's response to the growing economic influence of large digital platforms capable of controlling the access of economic entities to digital markets, online advertising, search engines, mobile operating platforms and e-commerce services (Bergkamp, 2021).

The legal framework established by the Digital Markets Act is based on the special status of large digital platforms, designated as "gatekeepers". According to Article 3 of the Regulation (EU) No. 2022/1925 of the European Parliament and of the Council[7], such entities are defined as companies that exert influence on

[1] General Agreement on Tariffs and Trade (GATT 1947). (1947, October). Retrieved from https://www.wto.org/english/docs_e/legal_e/downloads_e/GATT1947_en.pdf.
[2] General Agreement on Trade in Services. (1994, April). Retrieved from https://jusmundi.com/en/document/treaty/en-general-agreement-on-trade-in-services-1994-general-agreement-on-trade-in-services-1994-friday-15th-april-1994.
[3] Agreement on Trade-Related Aspects of Intellectual Property Rights. (1994, April). Retrieved from https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[4] Consolidated version of the Treaty on the Functioning of the European Union. (2012, October). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.
[5] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.
[6] Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
[7] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.

the internal market of the European Union, ensure the functioning of core platform services, and have an established market position. The criteria for determining "gatekeepers" include the company's annual turnover, market capitalisation, number of platform users, and the scale of digital service provision in EU Member States. Thus, European law links the application of special regulatory mechanisms not only to the fact of violation of competition law, but also to the entity's sustained ability to exert structural influence on the functioning of the digital market (Skara *et al*., 2024).

Unlike the Regulation (EU) No. 2022/1925 of the European Parliament and of the Council[1], which focuses on regulating the market power of large platforms, the Regulation (EU) No. 2022/2065 of the European Parliament and of the Council[2] aims to ensure the transparency of digital services and limit the spread of illegal content in the digital environment. This act establishes obligations for digital platforms to ensure the transparency of recommendation algorithms, disclose information about advertising mechanisms, and remove illegal content. At the same time, the Digital Services Act strengthens requirements for managing systemic risks associated with the operation of large online platforms, including the risks of information manipulation, restrictions on economic entities' access to digital services, and the unfair use of algorithms.

As a result, the application of European Union competition law began to cover not only classic forms of abuse of dominance, but also the use of digital infrastructure to create structural advantages for the platforms' own services. Antimonopoly control focused on mechanisms for providing priority access to platform services, the use of user data to enhance market power, limiting the compatibility of digital applications, and creating a dependent position of economic entities on the platform ecosystem. It is in this context that the European Commission initiated investigations against Google LLC, Apple Inc., Amazon.com, Inc., and Meta Platforms, Inc., considering the activities as potentially restricting competition in digital markets (Table 2).

Table 2. The European Commission's antitrust enforcement practices in relation to digital platforms in 2019-2024

Company	Object of antimonopoly control	Subject of legal assessment by the European Commission	Normative and legal significance for the development of competition law
Google	Search engines, Android, digital advertising	Using ranking algorithms to favour proprietary services; restricting competitors' access to the advertising infrastructure and Android mobile ecosystem	Expanding the category of abuse of a dominant position to the sphere of algorithmic governance of digital markets; developing an approach to regulating platform ecosystems
Apple	App Store and the iOS operating system	Restricting the use of alternative payment systems and distribution of applications outside the App Store	Developing an approach to ensuring non-discriminatory access of business entities to digital infrastructure and limiting closed digital ecosystems
Amazon	E-commerce and marketplaces	Using third-party merchant data to gain competitive advantages for its own services	Expanding the scope of competition law to regulate the use of commercial data and control of platform infrastructure
Meta	Social media and digital advertising	Pooling user data across platforms and leveraging digital infrastructure to enhance market concentration	Forming a link between competition regulation, personal data protection and limiting digital concentration

Source: compiled by the author based on Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising (2019), Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices (2020), Antitrust: Commission sends Statement of Objections to Apple on App Store rules for music streaming providers (2021), Directorate-General for Competition & Directorate-General for Communications Networks, Content and Technology (2024)

An analysis of the investigations presented in the table shows that the European Commission's practice shifted in its approach to determining the market power of economic entities. Under classical competition law, dominant position was associated with market share, price control, and the ability to restrict competition by changing the conditions of circulation of goods or services. In the digital economy, the ability of platforms to control digital infrastructure, manage ranking algorithms, accumulate user data, and determine the conditions of market participants' access to digital services became the object of legal assessment (Podszun *et al*., 2021). This demonstrates the expansion of the concept of dominant position and the adaptation of competition law to the platform economic model. The European Commission's practice also

[1] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.

[2] Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

demonstrates a shift in approaches to understanding anticompetitive behaviour. While previously, violations of competition law were associated with the actual restriction of competition, in the modern environment, the very ability of a digital platform to create structural advantages for its own services even before negative market consequences arise is becoming the subject of legal analysis (Crémer *et al*., 2019). As a result, the modern European model of competition regulation is shifting from reactive antimonopoly control to preventive regulation of digital markets, based on preventing the risks of monopolisation of digital infrastructure.

Constitutional and legal framework for regulating competition and restricting monopolistic activity in the Republic of Azerbaijan. The constitutional and legal framework for regulating competition in the Republic of Azerbaijan evolved amid the transformation of the economic system, the transition to market-based economic mechanisms, and the development of the private sector after independence. The changing structure of economic relations necessitated the normative consolidation of the principles of free entrepreneurship, equality of ownership, and the restriction of monopolistic activity as elements of a functioning market economy. These processes influenced the formation of the constitutional and legal framework for regulating competition and the development of state control mechanisms to limit monopolisation in individual sectors of the economy (Aghayev, 2023).

The legal framework for regulating economic relations in the Republic of Azerbaijan is the Constitution of the Republic of Azerbaijan[1], which enshrines the principles of economic freedom, diversity of ownership, and state guarantees for entrepreneurial activity. In accordance with Article 15 of the Constitution, economic development is based on various forms of ownership and serves to improve the well-being of the people. At the same time, Article 59 enshrines the right of everyone to freely use the resources and property to conduct entrepreneurial activity in accordance with the procedure established by law. These provisions form the constitutional basis for the functioning of a market economy and define the limits of state intervention in economic activity. Constitutional guarantees of freedom of economic activity in Azerbaijan are interrelated with the principle of equal protection of all forms of ownership and the need to ensure fair conditions for economic activity. In this context, constitutional and legal regulation of competition is aimed not only at ensuring freedom of entrepreneurship,but also at preventing the abuse of economic freedom through market monopolisation and restrictions on competition. Thus, the constitutional norms of the Republic of Azerbaijan provide for a combination of two interrelated elements: guarantees of economic initiative for business entities and the permissibility of state regulation to protect the competitive environment. This approach is consistent with modern trends in the constitutionalisation of competition law, in which the protection of competition is viewed as one of the mechanisms for ensuring economic balance and limiting the excessive concentration of economic power (OECD-GVH Regional Centre for Competition in Budapest, 2024).

It should be noted that the constitutional provisions of the Republic of Azerbaijan are not limited to enshrining freedom of entrepreneurship. In accordance with Article 15 of the Constitution of the Republic of Azerbaijan[2], the state guarantees economic development based on various forms of ownership and free enterprise, while simultaneously taking measures to prevent monopoly and unfair competition in economic relations. In this context, the provisions of the Competition Code of the Republic of Azerbaijan[3] serve as a normative mechanism for implementing constitutional provisions, specifying procedures for preventing monopolistic activity, controlling economic concentration, limiting the abuse of a dominant position, and combating unfair competition. Thus, the Code ensures the practical implementation of the constitutional principle of combining freedom of entrepreneurship with the state's obligation to maintain a competitive environment and prevent excessive concentration of economic power.

In the system of previously existing legislation, Law of the Republic of Azerbaijan No. 526 "On Anti-Monopoly Activities"[4] was adopted. The law regulated issues related to the abuse of a dominant position, price-fixing agreements, and other forms of anticompetitive behaviour. However, the law's content was based on approaches characteristic of the early stages of post-Soviet economic transformation, when competition regulation was viewed as a mechanism for administratively limiting the monopolisation of individual product markets. As a result, legal regulation focused on curbing existing violations, while mechanisms for preventive control of economic concentration and the prevention of structural restrictions on competition remained limited. Additional regulation was implemented through Law of the Republic of Azerbaijan No. 1049 "On Unfair Competition"[5], which prohibited the dissemination of false information, unfair advertising, misuse of business reputation, and other forms of unfair behaviour by business entities.

[1] Constitution of the Republic of Azerbaijan. (1995, November). Retrieved from https://president.az/en/pages/view/azerbaijan/constitution.
[2] Ibidem, 1995.
[3] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.
[4] Law of the Republic of Azerbaijan No. 526 "On Anti-Monopoly Activities". (1993, March). Retrieved from https://wipolex-res.wipo.int/edocs/lexdocs/laws/az/az/az025az.pdf?last-modified=1305040098&.
[5] Law of the Republic of Azerbaijan No. 1049 "On Unfair Competition". (1995, June). Retrieved from https://wipolex-res.wipo.int/edocs/lexdocs/laws/az/az/az125az_1.pdf?last-modified=1765787537&Expires=1782371184&Signature=pEvv8vBGlx~.

Unfair competition occupied a distinct place in the system of competition legislation in the Republic of Azerbaijan, as it was aimed not so much at limiting the market power of individual business entities as at ensuring fair conditions for conducting business activities. Manifestations of unfair competition included the dissemination of false information about competitors, misleading consumers about the characteristics of goods and services, the misuse of the goodwill of other business entities, and the creation of unjustified competitive advantages. The legal significance of regulating unfair competition lay in protecting both the interests of bona fide market participants and the interests of consumers, as such actions can distort the conditions of competition even in the absence of a dominant market position. Unlike mechanisms for combating monopolistic activity, which focused on controlling economic concentration and abuse of market power, unfair competition regulations were aimed at preventing unlawful competitive practices and restoring a level playing field.

At the same time, the Law of the Republic of Azerbaijan No. 590-IQ "On Natural Monopolies"[1] established the specifics of state regulation in areas where objective economic conditions limited the formation of a competitive environment. However, these legal acts functioned largely autonomously, leading to the fragmentation of competition regulation and the absence of a unified mechanism for the legal assessment of anticompetitive behaviour. In practice, this created difficulties in delineating the competence of antimonopoly authorities, defining the criteria for a dominant position, and applying mechanisms for controlling economic concentration.

The adoption of the Competition Code of the Republic of Azerbaijan[2] became one of the instruments for implementing the constitutional requirement to prevent monopoly and unfair competition, enshrined in Article 15 of the Constitution of the Republic of Azerbaijan[3]. Unlike the previous regulatory system, which relied on the autonomous regulation of individual areas of competition policy, the new Code created a unified system of legal regulation of competition, including mechanisms for controlling economic concentration, limiting monopolistic activity, and preventing unfair competition.

The inclusion of provisions on unfair competition in the Competition Code of the Republic of Azerbaijan[4] demonstrates the integration of this institution into a unified system of competition regulation. While these relations were previously regulated by a separate legislative act, unfair competition is now considered an independent form of disruption of the competitive environment, along with abuse of a dominant position and anticompetitive agreements. This approach ensures the application of unified mechanisms for the legal assessment of anticompetitive behaviour and allows for the consideration of the impact of unfair competitive practices on the competitive environment. The Code provides for a set of measures aimed at ending violations of competition law, preventing restrictions on competition, and protecting the legitimate interests of market participants. In order to compare the provisions of the Competition Code of the Republic of Azerbaijan with international and supranational approaches to competition regulation, the provisions governing the definition of a dominant position and abuse of market power (Articles 15-16 of the Code), economic concentration and the procedure for its state control (Articles 26-31 of the Code), unfair competition (Articles 18-22 of the Code), the powers of the competition authority and control procedures (Articles 43-61 of the Code), as well as measures of liability for violation of competition legislation (Articles 74-84 of the Code) were analysed (Table 3).

Table 3. Comparison of the provisions of the Competition Code of the Republic of Azerbaijan with international and supranational approaches to competition regulation

Element of international standards	Implementation in the Competition Code of Azerbaijan	Existing limitations and problems
Comprehensive regulation of competitive relations	The Code combined the regulation of monopolistic activity, unfair competition and economic concentration	The mechanisms of interaction between individual competition law institutions require further detailing
Preventive control of economic concentration	Preliminary review procedures for mergers and acquisitions were introduced.	There are no detailed criteria for assessing the permissibility of concentration
Expanded understanding of dominant position	The possibility of the subject's influence on the conditions of circulation of goods and access to markets is taken into account	The level of evaluation categories in determining market power remains high
Integration of unfair competition into the antimonopoly control system	Unfair competition is considered as an element of restricting the competitive environment	Mechanisms for combating digital forms of unfair competition are insufficiently regulated
Strengthening the powers of the antimonopoly authority	Expanded powers to conduct investigations and control concentrations	The risk of excessive discretion on the part of the antimonopoly authority remains

[1] Law of the Republic of Azerbaijan No. 590-IQ "On Natural Monopolies". (1998, December). Retrieved from http://binegedi-ih.gov.az/storage/files/files/15_12_1998%20-%20T%C9%99bii%20inhisarlar%20%20haqq%C4%B1nda%20Az%C9%99rbaycan%20Respublikas%C4%B1n%C4%B1n%20Qanunu.pdf.
[2] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.
[3] Constitution of the Republic of Azerbaijan. (1995, November). Retrieved from https://president.az/en/pages/view/azerbaijan/constitution.
[4] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.

Table 3, Continued

Element of international standards	Implementation in the Competition Code of Azerbaijan	Existing limitations and problems
Adaptation to the digital economy	The Code contains general mechanisms for assessing market power and economic concentration that could potentially be applied to digital markets, but does not provide for specific rules on digital platforms	There are no special mechanisms for regulating digital platforms under the Digital Markets Act model/Digital Services Act model
Harmonisation with international standards	Separate approaches of the OECD and the European Union are used	The implementation of international standards remains incomplete and depends on law enforcement practices

Source: compiled by the author based on General Agreement on Tariffs and Trade (GATT 1947)[1]; General Agreement on Trade in Services[2]; Agreement on Trade-Related Aspects of Intellectual Property Rights[3]; Regulation (EU) No. 2022/1925 of the European Parliament and of the Council[4]; Regulation (EU) No. 2022/2065 of the European Parliament and of the Council[5]; Competition Code of the Republic of Azerbaijan[6]

A comparison of the provisions of the Competition Code of the Republic of Azerbaijan[7] with international approaches to competition regulation reveals a change in the structure of national competition legislation. While antitrust regulation was previously focused primarily on preventing individual violations of competition law, the Competition Code provides for the interrelated regulation of economic concentration, dominant position, and unfair competition within a unified system of antimonopoly control. As a result, the scope of legal regulation was expanded to include mechanisms for preventing restrictions on competition and assessing the impact of economic entities on the competitive environment.

A comparative analysis of the Code's provisions reveals that certain competition regulation mechanisms were developed taking into account the approaches of the OECD and the European Union. This is reflected in the expansion of the criteria for determining a dominant position, the use of mechanisms for preliminary control of economic concentration, and the integration of unfair competition regulation into the antimonopoly control system. In contrast to the Law of the Republic of Azerbaijan No. 526[8], which primarily linked a dominant position to an economic entity's share of the relevant product market, the Competition Code of the Republic of Azerbaijan[9] provides for a broader approach to assessing market power. In addition to quantitative indicators, the Code takes into account an economic entity's ability to influence the conditions of product circulation, market access, and the state of the competitive environment, which is consistent with modern OECD and European Union approaches to assessing companies' market power.

At the same time, an analysis of the Competition Code reveals the persistence of a number of problems related to the level of legal certainty within certain competition regulation mechanisms. Specifically, the Code's provisions governing the control of economic concentration stipulate the need to assess the impact of relevant transactions on competition and the potential for significant restrictions on market competition. However, these provisions do not contain detailed criteria for determining the permissible level of concentration or a methodology for assessing its consequences for individual product markets. Similarly, the Code's provisions devoted to defining a dominant position allow for the consideration of a business entity's ability to influence the conditions of product circulation and market access. However, specific indicators of such market power are formulated primarily through evaluative categories. Some provisions of the Code rely on the concepts of "significant restriction of competition", "market influence", and "dominant position", the meaning of which is subject to interpretation by the competent competition authority. As a result, a significant amount of authority to assess the consequences of economic concentration, determine the presence of a

[1] General Agreement on Tariffs and Trade (GATT 1947). (1947, October). Retrieved from https://www.wto.org/english/docs_e/legal_e/downloads_e/GATT1947_en.pdf.
[2] General Agreement on Trade in Services. (1994, April). Retrieved from https://jusmundi.com/en/document/treaty/en-general-agreement-on-trade-in-services-1994-general-agreement-on-trade-in-services-1994-friday-15th-april-1994.
[3] Agreement on Trade-Related Aspects of Intellectual Property Rights. (1994, April). Retrieved from https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[4] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.
[5] Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
[6] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.
[7] Ibidem, 2023.
[8] Law of the Republic of Azerbaijan No. 526 "On Anti-Monopoly Activities". (1993, March). Retrieved from https://wipolex-res.wipo.int/edocs/lexdocs/laws/az/az/az025az.pdf?last-modified=1305040098&.
[9] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.

dominant position, and qualify restrictions on competition is concentrated within the purview of the antimonopoly authority. In this regard, procedural guarantees for market participants require further improvement, including more detailed regulatory codification of decision-making criteria, unification of investigation procedures, and the development of mechanisms for judicial review of decisions by the competition regulator. As a result, the practical application of individual provisions of the Code will depend on the development of uniform administrative and judicial practice.

The adoption of the Competition Code of the Republic of Azerbaijan is associated with a transition to a more systemic model of competition regulation and the expansion of antimonopoly control mechanisms. At the same time, an analysis of the provisions of the Code and international competition regulation practices makes it possible to identify several areas for further improvement of the competition legislation of the Republic of Azerbaijan. Taking into account the approaches of the OECD and the European Union, it seems appropriate to develop more detailed criteria for assessing a dominant position and the permissibility of economic concentration, including methodologies for analysing the influence of economic entities on digital markets, platform infrastructure, and access to user data. Mechanisms for monitoring the activities of digital platforms require additional regulatory oversight, as Azerbaijan's current legislation is primarily focused on traditional commodity markets and does not provide for specific mechanisms for regulating platform dependence and algorithmic market governance. A comparative analysis also demonstrates the feasibility of further harmonising the competition legislation of the Republic of Azerbaijan with the preventive antimonopoly control mechanisms used in the European Union. In particular, a prospective direction could be the development of mechanisms for preliminary assessment of competition risks in the digital sector, as well as the introduction of special regulations for entities with significant infrastructural influence on digital markets. These measures will allow national competition legislation to adapt to changes in the structure of economic relations and increasing digital concentration.

Discussion

The results of the study demonstrate that the modern international anti-monopoly model is gradually shifting from a predominantly reactive approach to suppressing competition law violations to the use of preventive mechanisms for controlling restrictions on competition. This conclusion aligns with the position of J. Tirole (2023), who noted the transformation of traditional notions of market power and the need to adapt competition regulation to new economic conditions. At the same time, the study also demonstrated that the development of international competition protection mechanisms is associated not only with the refinement of tools for controlling individual violations but also with the expansion of opportunities to prevent competition restrictions at the early stages of the emergence. This makes it possible to consider modern antitrust mechanisms as an element of ensuring a balanced relationship between freedom of entrepreneurship and public interests in the protection of competition.

The analysis also revealed that the development of competition law is characterised by a strengthening of the role of preventive control and an expansion of the powers of competition regulators. Similar conclusions are presented in the work of V.H.S.E. Robertson (2024), who demonstrates that modern competition regulation mechanisms are aimed at preventing the risks of restricting competition before significant negative consequences for the market arise. The results of this study further demonstrate that the expansion of supervisory powers requires maintaining a balance between the effectiveness of antitrust regulation and compliance with the principles of legal certainty, particularly when using the assessment criteria for determining market power and restricting competition.

The results of the study indicate that the development of the Digital Markets Act[1] is associated with a change in the approach to determining the dominant position of economic entities in the digital economy. This conclusion partially coincides with the findings of I. Daems (2022), who concluded that the practical implementation of the new digital regulation of the European Union is highly complex due to the combination of antitrust and administrative control mechanisms. The study confirms that the criteria for defining "gatekeepers", including the size of the user base, the scale of digital services, and the sustainability of infrastructural influence, expand the scope of the category of market power compared to traditional competition law. At the same time, the results of the analysis suggest that the main challenge in applying the Digital Markets Act is related not only to the technical complexity of implementing new regulatory mechanisms, as emphasised by I. Daems, but also to the lack of unified international approaches to assessing digital concentration and the business entities' dependence on platforms.

The study demonstrated that the constitutional and legal model for regulating competition in the Republic of Azerbaijan is based on a combination of freedom of entrepreneurship and the permissibility of state intervention to prevent monopoly and unfair

[1] Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)". (2022, September). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/1925/oj.

competition. An analysis of Article 15 of the Constitution of the Republic of Azerbaijan[1] and the provisions of the Competition Code of the Republic of Azerbaijan[2] make it possible to consider the protection of competition as one of the mechanisms for implementing constitutional guarantees of economic freedom. The obtained results are consistent with the findings of U. Aydin (2026), according to which, in states undergoing processes of political and economic transformation, competition law performs not only a regulatory function, but also helps to limit the excessive concentration of economic power and maintain an institutional balance between the state and business entities.

The results of the study demonstrate that constitutional and legal regulation of competition in the Republic of Azerbaijan is gradually shifting from formal restrictions on monopolistic activity to more comprehensive control of market concentration and the influence of economic entities on the competitive environment. Similar conclusions are presented in the work of A. Gawer & C. Bonina (2024), which found that the development of digital platforms in countries with transition and developing economies is accompanied by increasing market infrastructural dependence on a limited number of large digital intermediaries. At the same time, the study additionally revealed that for the Republic of Azerbaijan, the problem lies not only in the growth of digital concentration but also in the preservation of the regulatory orientation of competition law primarily toward traditional product markets. In contrast to the position of A. Gawer & C. Bonina, which focused primarily on the economic consequences of platform dominance, the results of the study also made it possible to identify constitutional and legal limitations on the adaptation of antitrust regulation to the digital economy. A comparative analysis revealed that Azerbaijan's current competition regulation system includes certain elements of preventive antimonopoly control, but maintains a high level of administrative discretion in determining market power criteria. A similar trend is also evident in the study by K.J. Cseres (2021), who substantiated that the interaction between competition regulation and administrative mechanisms for controlling dominance is accompanied by an expansion of the discretionary powers of competition oversight bodies. The study confirmed that the use of evaluative categories in determining "significant restriction of competition" or "market influence" can complicate the development of uniform enforcement practice. However, in contrast to the findings of K.J. Cseres, the study found that in the Republic of Azerbaijan, this problem is further exacerbated by the lack of detailed methodologies for assessing digital market concentration and business entities' dependence on platforms.

The study concluded that Azerbaijan's current competition legislation is partially guided by international standards for protecting economic freedom, limiting monopolistic activity, and ensuring fair competition. At the same time, problems remain related to the level of legal certainty of individual mechanisms for controlling economic concentration, determining a dominant position, and exercising the powers of the antimonopoly authority. Similar results are presented in the work of B.N.P. Panda (2025), which establishes that the effective protection of economic freedom requires the formation of transparent legal mechanisms for competition regulation and the prevention of excessive concentration of market power. At the same time, the conducted study showed that for the Republic of Azerbaijan, the improvement of competition legislation is associated not only with the further harmonisation of national norms with international approaches, but also with the need to strengthen institutional guarantees for the protection of competition in the context of economic transformation. In contrast to the approach of B.N.P. Panda, which focuses primarily on certain areas of competition regulation development, the results of the study make it possible to consider the protection of the competitive environment as an element of the implementation of constitutional guarantees of freedom of entrepreneurship and ensuring a balance between the economic freedom of business entities and the permissible limits of state intervention in economic relations.

The study's findings also demonstrate that the effectiveness of antitrust regulation is determined not only by the content of specific competition law provisions but also by the compliance with constitutional guarantees of economic freedom and legal certainty. It was established that the development of mechanisms to control economic concentration and dominant positions should be accompanied by ensuring the predictability of state regulation and procedural guarantees for market participants. Similar patterns were identified by E. Carbonara & E. Santarelli (2023), who concluded that there is a stable relationship between the level of constitutional protection of economic rights, the development of entrepreneurial activity, and the quality of the competitive environment. The findings are consistent with those of A. Huseynov *et al*. (2025), who found that the development of Azerbaijan's digital economy is accompanied by persistent structural limitations to digital competitiveness and requires further improvement of state regulation mechanisms. The authors noted the need to leverage advanced international practices to improve the effectiveness of the digital transformation of the economy. E.R. Banalieva & C. Dhanaraj (2019) argued that the digital economy challenged traditional assumptions of internalisation theory, as digital

[1] Constitution of the Republic of Azerbaijan. (1995, November). Retrieved from https://president.az/en/pages/view/azerbaijan/constitution.
[2] Competition Code of the Republic of Azerbaijan. (2023, December). Retrieved from https://e-qanun.az/framework/56187.

platforms, data flows, and network effects transformed the way companies organise the international operations. The authors demonstrated that digitalisation reduced certain transaction costs but simultaneously created new strategic challenges related to control, scalability, data ownership, and coordination across markets.

Thus, the results of this study demonstrate the development of international and national competition regulation mechanisms toward strengthening preventive antimonopoly control, improving mechanisms for preventing economic concentration, and ensuring a balance between freedom of entrepreneurship and public interests in protecting competition. A comparison of the obtained results with scientific research confirmed the need to further refine the competition legislation of the Republic of Azerbaijan, enhance the legal certainty of antimonopoly control mechanisms, and strengthen constitutional guarantees for protecting the competitive environment.

Conclusions

The study revealed that countering monopolism in the Republic of Azerbaijan has constitutional and legal significance and is linked to the implementation of the principles of freedom of entrepreneurship, fair competition, and equality of economic participants. An analysis of the Constitution of the Republic of Azerbaijan revealed that the protection of competition is viewed not only as a direction of state economic policy, but also as a mechanism for ensuring the effective functioning of a market economy.

It was established that the adoption of the Competition Code of the Republic of Azerbaijan marked a stage in the modernisation of national competition legislation. Unlike the previously existing regulations, the Code established a comprehensive system of legal regulation covering issues of dominance, economic concentration, and unfair competition. A comparative-legal analysis revealed the expansion of mechanisms for preliminary control of economic concentration and the use of a broader approach to assessing the market power of business entities.

The results of the study indicate partial implementation of international standards of competition regulation. At the same time, the national model retains its own characteristics, determined by the specifics of the legal system and the objectives of economic development in the Republic of Azerbaijan. It was established that current legislation creates the legal preconditions for preventing anticompetitive behaviour and limiting excessive concentration of economic power; however, certain mechanisms require further improvement.

Prospective areas for the development of competition law include clarifying the criteria for assessing dominant positions and economic concentration, improving the regulation of digital markets and platforms, specifying the assessment categories of competition law, and strengthening procedural guarantees for business entities and mechanisms for judicial review of decisions of the antimonopoly authority. Implementation of these measures will ensure a more consistent implementation of the constitutional principles of freedom of entrepreneurship, fair competition, and the prevention of monopolistic activity in law enforcement practice in the Republic of Azerbaijan.

The limitations of the study are related to the regulatory nature of the analysis conducted. The study was based on an analysis of constitutional provisions, national competition legislation of the Republic of Azerbaijan, and international legal acts, without conducting an independent empirical analysis of statistical data on the state of the competitive environment and market concentration. Prospects for further research include studying the practice of applying the Competition Code of the Republic of Azerbaijan, analysing the formation of administrative and judicial practice in the field of competition protection, and assessing the effectiveness of legal mechanisms for controlling economic concentration and limiting the abuse of market power.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Abdullayev, K., Abdullayev, R., Yusifov, E., Babazade, I., & Fataliyeva, G. (2024). Main areas of development of the digital economy in the Republic of Azerbaijan. *Economics of Development,* 23(1), 78-88. doi: 10.57111/econ/1.2024.78.

[2] Aghayev, R. (2023). *Will Azerbaijan's Competition Code be a tool for a highly monopolized economy?* Retrieved from https://bakuresearchinstitute.org/en/will-azerbaijans-competition-code-be-a-tool-for-a-highly-monopolized-economy/.

[3] Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising. (2019). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

[4] Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices. (2020). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077.

[5] Antitrust: Commission sends Statement of Objections to Apple on App Store rules for music streaming providers. (2021). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061.
[6] Aydin, U. (2026). Competition law and transitions to and away from democracy. *European Law Journal,* 32(1), 26-37. doi: 10.1111/eulj.70017.
[7] Bakalinska, O., Honcarenko, O., Kaptsova, T., & Babadzhanian, H. (2022). Advocacy of competition in the world and Ukraine: Comparative characteristics. *Access to Justice in Eastern Europe*, 4(16), 145-158. doi: 10.33327/ajee-18-5.4-n000428.
[8] Banalieva, E.R., & Dhanaraj, C. (2019). Internalization theory for the digital economy. *Journal of International Business Studies,* 50(8), 1372-1387. doi: 10.1057/s41267-019-00243-7.
[9] Bergkamp, P.A. (2021). The proposed EU Digital Markets Act: A new era for the digital economy in Europe. *European Company Law,* 18(5), 152-161. doi: 10.54648/eucl2021020.
[10] Bernatt, M. (2025). Competition law through the lenses of national constitutions: Connecting competitive markets with socio-economic and environmental values. *Journal of Antitrust Enforcement,* 13(2), 284-314. doi: 10.1093/jaenfo/jnae047.
[11] Carbonara, E., & Santarelli, E. (2023). The impact of constitutional protection of economic rights on entrepreneurship: A taxonomic survey. *Foundations and Trends in Entrepreneurship,* 19(2), 126-223. doi: 10.1561/0300000105.
[12] Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration,* 44(1), 41-57. doi: 10.1080/07036337.2021.2011260.
[13] Crémer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition policy for the digital era*. Luxembourg: Publications Office of the European Union. doi: 10.2763/407537.
[14] Cseres, K.J. (2021). Intersection of competition and regulation in abuse of dominance and monopolization. *Amsterdam Law School Legal Studies Research Paper No. 2021-36; Amsterdam Centre for European Law and Governance Research Paper No. 2021-03.*
[15] Daems, I. (2022). The complexity and practical challenges of implementing the new DMA. *Competition Law & Policy Debate,* 7(3), 106-112. doi: 10.4337/clpd.2022.03.01.
[16] Directorate-General for Competition, & Directorate-General for Communications Networks, Content and Technology. (2024). *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act*. Retrieved from https://surl.li/wzqklv.
[17] Fazio, E. (2022). Adapting competition law to the digital transition. Two challenges. *European Papers,* 7(3), 981-992. doi: 10.15166/2499-8249/601.
[18] Gawer, A., & Bonina, C. (2024). Digital platforms and development: Risks to competition and their regulatory implications in developing countries. *Information and Organization,* 34(3), article number 100525. doi: 10.1016/j.infoandorg.2024.100525.
[19] Guliyeva, A. (2025). State support for entrepreneurship in Azerbaijan, 2020-2025: Policies, programs, and outcomes. *Gate of the Universes,* 1(7), 94-103. doi: 10.69760/portuni.0107008.
[20] Guluzade, T. (2025). Development prospects of the digital economy in Azerbaijan. *Gate of the Universes,* 1(7), 51-59. doi: 10.69760/portuni.0107006.
[21] Huseynov, A., Balsalobre-Lorente, D., Hamidova, L., & Samedova, E. (2025). Challenges and opportunities of digital economy development: Case of Azerbaijan. *Problems and Perspectives in Management,* 23(2), 265-276. doi: 10.21511/ppm.23(2).2025.18.
[22] Khalilov, A. (2024). The concept and essence of the principle of subsidiarity in the field of constitutional law in the Republic of Azerbaijan. *European Law Science,* 1, 21-24. doi: 10.32782/chern.v1.2024.4.
[23] Kovacic, W.E., & Shapiro, C. (2000). Antitrust policy: A century of economic and legal thinking. *Journal of Economic Perspectives,* 14(1), 43-60. doi: 10.1257/jep.14.1.43.
[24] OECD-GVH Regional Centre for Competition in Budapest. (2024). *Competition policy in Eastern Europe and Central Asia: Advocacy of competition*. Retrieved from *https://surl.li/cjwhih*.
[25] Organisation for Economic Co-operation and Development. (2024). *Competition policy in digital markets: The combined effect of ex ante and ex post instruments in G7 jurisdictions*. doi: 10.1787/80552a33-en.
[26] Organisation for Economic Co-operation and Development. (2025). *Recommendation of the Council concerning effective action against hard core cartels*. Retrieved from https://surl.li/esowoy.
[27] Panda, B.N.P. (2025). Economic liberty in digital market and digital competition legislation: Indian context. *Law and World,* 11(35), 1-11. doi: 10.36475/11.3.1.
[28] Podszun, R. (2023). From competition law to platform regulation – regulatory choices for the digital markets act. *Economics,* 17(1), article number 20220037. doi: 10.1515/econ-2022-0037.
[29] Podszun, R., Bongartz, P., & Langenstein, S. (2021). The digital markets act: Moving from competition law to regulation for large gatekeepers. *Journal of European Consumer and Market Law,* 10(2), 60-67.

[30] Robertson, V.H.S.E. (2024). The complementary nature of the Digital Markets Act and the EU antitrust rules. *Journal of Antitrust Enforcement,* 12(2), 325-330. doi: 10.1093/jaenfo/jnae013.
[31] Skara, G., Muçollari, O., & Hajdini, B. (2024). Adapting the competition policy for the digital age: assessing the EU's approach. *Laws,* 13(5), article number 64. doi: 10.3390/laws13050064.
[32] Tirole, J. (2023). Competition and the industrial challenge for the digital age. *Annual Review of Economics,* 15, 573-605. doi: 10.1146/annurev-economics-090622-024222.
[33] United Nations Conference on Trade and Development. (2000). *The United Nations set of principles and rules on competition*. Retrieved from https://unctad.org/system/files/official-document/tdrbpconf10r2.en.pdf.
[34] United Nations Conference on Trade and Development. (2024). *Enforcing competition law in digital markets and ecosystems: Policy challenges and options*. Retrieved from https://surl.li/nurgyo.

Конституційно-правові аспекти вдосконалення механізму протидії монополізму та недобросовісній конкуренції

Мурад Оруджов
Магістр, докторант, старший спеціаліст з контрактів
Національна авіаційна академія
AZ1045, просп. Мардакан, 30, м. Баку, Азербайджан
https://orcid.org/0009-0002-7169-8453

Анотація
Метою дослідження було визначення напрямів удосконалення конституційно-правових механізмів протидії монополізму та недобросовісній конкуренції. Були використані формально-правові, порівняльно-правові, тематичні дослідження та методи правового моделювання. Дослідження продемонструвало, що конституційно-правова модель регулювання конкуренції в Азербайджанській Республіці базується на поєднанні гарантій свободи підприємництва та допустимості державного втручання для обмеження монополістичної діяльності. Встановлено, що попередня система антимонопольного регулювання, створена між 1993 і 1998 роками, характеризувалася фрагментарним правовим регулюванням, недостатньою координацією механізмів контролю за економічною концентрацією, домінуючим становищем та недобросовісною конкуренцією, а також була спрямована на припинення наявних порушень. У дослідженні обґрунтовано необхідність удосконалення правових механізмів запобігання антиконкурентній поведінці, посилення контролю за економічною концентрацією та адаптації конкурентного законодавства до умов цифрової економіки. Порівняльно-правовий аналіз чинного законодавства Азербайджанської Республіки, законодавства Європейського Союзу та міжнародних підходів до регулювання конкуренції продемонстрував перехід Азербайджану до системної моделі контролю конкуренції, яка передбачає взаємопов'язане регулювання економічної концентрації, домінування та недобросовісної конкуренції, а також часткове впровадження стандартів міжнародного конкурентного права. У порівняльному контексті встановлено, що міжнародні антимонопольні механізми еволюціонували від моніторингу картелів та зловживання домінуючим становищем до превентивного регулювання цифрових ринків та платформної економіки. З'ясовано, що Європейський Союз розробив специфічну модель регулювання цифрових платформ у 2020–2025 роках, поширивши антимонопольний контроль на алгоритмічне управління, використання даних користувачів та цифрову інфраструктуру. Результати дослідження можуть бути використані законодавчим органом Азербайджанської Республіки, органами, що реалізують державну конкурентну політику та антимонопольний контроль, та академічними установами для вдосконалення конкурентного законодавства, розробки механізмів регулювання цифрових ринків та підготовки пропозицій щодо гармонізації національної системи антимонопольного контролю з міжнародними стандартами конкурентного права

Ключові слова:
економічна концентрація; домінуюче становище; ринкова влада; цифрові платформи; міжнародні стандарти

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

Науковий журнал

Том 16, № 2, 2026

Заснований 2011 року. Виходить чотири рази на рік

Оригінал-макет видання виготовлено у відділі організації наукової діяльності
Національної академії внутрішніх справ

Відповідальний редактор:
Я. Шумко

Підписано до друку 26 травня 2026 р. Формат 60*84/8
Умов. друк. арк. 10,6
Наклад 50 прим.

Адреса видавництва:
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
Тел.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/uk

LAW JOURNAL
OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS

Scientific Journal

Volume 16, No. 2, 2026

Founded in 2011. Published four times per year

The original layout of the publication is made in the Department of Organisation of Scientific Activity of National Academy of Internal Affairs

Managing editor:
Ya. Shumko

Signed for print of May 26, 2026. Format 60*84/8
Conventional printed pages 10.6
Circulation 50 copies

Editors office address:
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
Tel.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/en