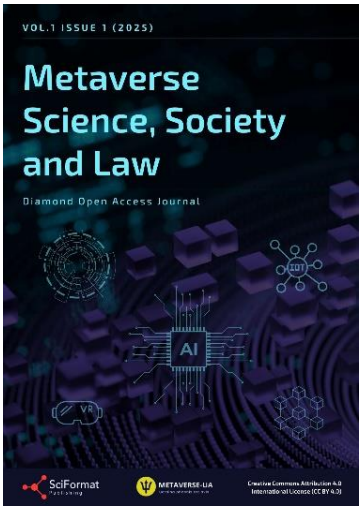

Metaverse Science, Society and Law

Vol. 1, Issue 1 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

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

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN ENSURING STATE SECURITY IN UKRAINE'S BORDER REGIONS BY LAW ENFORCEMENT AGENCIES
ARTICLE INFO	Oleksandr Nikitenko, Oleh Predmestnikov, Illia Zhuravel, Bohdan Krymchanin. (2025) Legal Regulation of The Use of Artificial Intelligence in Ensuring State Security in Ukraine's Border Regions by Law Enforcement Agencies. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.17
DOI	https://doi.org/10.69635/mssl.2025.1.1.17
RECEIVED	07 May 2025
ACCEPTED	15 July 2025
PUBLISHED	25 July 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN ENSURING STATE SECURITY IN UKRAINE'S BORDER REGIONS BY LAW ENFORCEMENT AGENCIES

Oleksandr Nikitenko
Doctor of Juridical Sciences, Academician of Administrative-Legal Sciences, Professor, Honored Lawyer of Ukraine, State Tax University, Ukraine
ORCID ID: 0009-0001-6572-4072

Oleh Predmestnikov
Doctor of Juridical Sciences, Professor, Honored Lawyer of Ukraine, Bogdan Khmelnitsky Melitopol State Pedagogical University, Ukraine
ORCID ID: 0000-0001-8196-647X

Illia Zhuravel
Postgraduate Researcher, Research Institute of Public Law, Ukraine
ORCID ID: 0009-0004-6486-6601

Bohdan Krymchanin
Third-Year Higher Education Student, University of the State Fiscal Service of Ukraine, Ukraine
ORCID ID: 0009-0003-4339-6658

ABSTRACT

This study is devoted to the legal regulation of artificial intelligence (AI) in ensuring state security in Ukraine's border regions amid global challenges, including cross-border crime, migration flows, and hybrid threats. In the context of Russia's full-scale war against Ukraine, launched on February 24, 2022, protecting the state border has become critically important for Ukraine's sovereignty and territorial integrity. The research explores the potential of AI for automating border control, verifying identities, detecting suspicious behavior, forecasting threats, and modeling security scenarios in the metaverse.
Through normative legal analysis, comparative methodology, and case studies, Ukrainian laws such as "On the State Border of Ukraine," "On the State Border Guard Service of Ukraine," and "On the Participation of Citizens in the Protection of Public Order and the State Border" were examined, revealing their inadequacy in regulating AI technologies. Based on the EU AI Act, the study proposes a legal model for the ethical implementation of AI that ensures rule of law, protection of human rights, and public trust.
The integration of AI with the metaverse opens new opportunities for training border guards, simulating hybrid threats, and optimizing resources - reducing risks during real-world operations. The findings support harmonization of Ukrainian legislation with European standards, strengthening border security, and promoting European integration. The research emphasizes the need for a comprehensive approach to conflict resolution, combining diplomatic, political, economic, and technological measures. It highlights the importance of ethical AI governance to ensure transparency, accountability, and the protection of citizens' constitutional rights, which is critical for Ukraine in the face of modern security challenges.

KEYWORDS

Border Security, Legal Regulation, Artificial Intelligence, Metaverse, State Security of Ukraine, Legal Governance

CITATION

Oleksandr Nikitenko, Oleh Predmestnikov, Illia Zhuravel, Bohdan Krymchanin. (2025) Legal Regulation of The Use of Artificial Intelligence in Ensuring State Security in Ukraine's Border Regions by Law Enforcement Agencies. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.17

Introduction.

In the good old days, it was said: when choosing a house, choose your neighbor first. Today, by virtue of history, Ukraine has become a neighbor in a complex geopolitical context, where the full-scale war launched by Russia on February 24, 2022, has underscored the critical importance of border security. Modern processes of European and global interdependence, the mutual penetration of cultural, political, economic, and socio-psychological ties - supported by new communication technologies - affect all European Union countries and, in particular, those areas related to border security.

For Ukraine, the protection of sovereignty and territorial integrity, as well as the provision of economic and informational security, are among the most important functions of the state and the responsibility of the entire Ukrainian people [1]. The maintenance of law and order in Ukraine is based on the principles of the rule of law, according to which no individual may be compelled to act unless provided for by legislation; citizens have equal constitutional rights and freedoms and are equal before the law. Ukrainians are guaranteed the right to peaceful assemblies, rallies, marches, and demonstrations without weapons [2].

The protection of the state border is regulated by a series of normative legal acts, in particular the Law of Ukraine "On the State Border of Ukraine" (1992) and the Law "On the State Border Guard Service of Ukraine" (2003). Since its independence, Ukrainian authorities have used administrative-legal instruments to regulate the treaty-based aspects of shared borders with neighboring countries, to ensure compliance with border regimes, and to strengthen border security [3]. In this context, the integration of innovative technologies - particularly artificial intelligence - is gaining increasing importance, allowing for improved border protection and timely responses to various types of threats.

Cross-border crime, illegal migration, hybrid threats, and cyberattacks require a comprehensive approach, combining diplomatic, political, economic, and technological measures. Artificial intelligence (AI) offers solutions for automating document verification, real-time data analysis, facial recognition, and threat forecasting.

The integration of AI with the metaverse enables virtual simulations for training border guards, increasing efficiency without risk. However, legislative gaps create legal uncertainty and ethical risks. This study seeks to answer the question: what legal and ethical mechanisms are necessary to regulate AI in Ukraine's border security domain, with integration of the metaverse?

Objective: To analyze the legislation, assess the potential of AI and the metaverse, and develop recommendations.

Scope: Ukrainian and international legislation, case studies, and virtual platforms.

Expected Contribution: Enhanced security, harmonization with European standards, and ethical governance.

The article is structured as follows: the literature review synthesizes sources; the methodology outlines approaches; the results present the analysis; the discussion interprets the data; and the conclusions provide recommendations.

Literature Review

The issue of legal regulation of the use of artificial intelligence (AI) in the field of state security in Ukraine's border regions is interdisciplinary, encompassing constitutional, administrative, informational, and service law. In the context of the full-scale war launched by Russia on February 24, 2022, border security has become a key factor in protecting Ukraine's sovereignty and territorial integrity, as well as ensuring its economic and informational security and the rule of law.

To identify priority directions and core tasks for the development of artificial intelligence, the Cabinet of Ministers of Ukraine approved the *Concept of Artificial Intelligence Development* on December 2, 2020, aiming to advance AI technologies in Ukraine as one of the priority areas in the field of scientific and technological research [4]

Ukrainian scholars, including V. Halunko and O. Pravotorova [22], emphasize the need to integrate AI into administrative and legal mechanisms for reforming border management, highlighting the importance of ethical principles and integrity. O. Nikitenko [3] identifies gaps in the coordination of law enforcement agencies in border regions, particularly under martial law, and calls for the development of legal norms governing AI.

International studies broaden the context. Ana Beduschi examines how artificial intelligence is used to manage international migration. She analyzes technologies applied for border control, identity verification, and automated decision-making for refugees and migrants. Her work also explores the ethical, legal, and political challenges involved, including risks of discrimination, human rights violations, and lack of algorithmic transparency [5].

Yiran Yang, Frederik Zuiderveen Borgesius, Pascal Beckers, and Evelien Brouwer have investigated the use of automated decision-making systems and AI at the borders of the European Union. They analyzed the impact of these technologies on human rights, particularly privacy, potential discrimination, and limited access to legal remedies. Their study concluded that automated systems at European borders pose significant human rights risks and require rigorous legal and ethical oversight [6].

Researchers from the Netherlands - Carolina La Fors and Fran Meissner - in their article *"Contesting Border Artificial Intelligence: Applying the Guidance-Ethics Approach as a Responsible Design Lens"* explored the use of AI in border control systems and assessed how ethical approaches can support more responsible technological design. Their conclusions stress that AI implementation at borders should be accompanied by clear ethical principles, interdisciplinary collaboration, and the involvement of all stakeholders to prevent discrimination, ensure transparency, and protect human rights [7].

Lyra, Damásio, Pinheiro, and Bacao [8] analyze AI applications for combating cross-border crime, focusing on predictive analytics and real-time monitoring. Frontex [9] describes the "Smart Borders" system, which uses AI for biometric verification and migration flow analysis, while also emphasizing the need for transparency, as outlined by the EU AI Act. This Act introduces a risk-based regulatory model for AI, prohibiting high-risk systems that violate human rights, such as social scoring [10].

Buolamwini and Gebru [11] warn of algorithmic bias in facial recognition systems, which may exacerbate discrimination at borders, especially in conflict regions.

The integration of artificial intelligence and metaverse technologies represents a new direction that significantly improves the quality and efficiency of training programs for the European Border and Coast Guard Agency. This integration enables realistic simulations of complex scenarios and enhances the adaptability of personnel training [12].

In their study, Lifelo, Ding, Ning, Qurat-Ul-Ain, and Dhelim [13] emphasize that integrating artificial intelligence and metaverse technologies opens new possibilities for creating adaptive and scalable training environments in the field of border security. These environments can simulate complex hybrid threats and improve training effectiveness - highly relevant to Ukraine's current challenges.

However, these studies do not address the specifics of Ukraine's wartime context, where hybrid threats complicate the implementation of AI technologies [14].

There are significant gaps in the literature. Ukrainian research [29, 31] focuses on general aspects of administrative law but fails to propose concrete AI regulatory models for border security in wartime conditions. International literature [8] overlooks Ukraine's unique context, particularly hybrid threats and martial law. Metaverse-related studies [12] remain limited to technical aspects, without analyzing legal or ethical regulation. The balance between AI efficiency and human rights protection remains a contentious issue, especially in border zones, where low public trust in surveillance technologies hinders implementation [25].

This study fits into the academic discourse by filling existing gaps through the analysis of the Laws of Ukraine "On the State Border" [16] and "On the State Border Guard Service" [32], revealing their inconsistency with the requirements for AI regulation. It evaluates the potential of artificial intelligence (AI) and the metaverse for automation, forecasting, and training, and proposes a legal model that incorporates the EU AI Act and ethical principles. The research contributes to discussions on the digital transformation of border security, harmonization with European standards, and the protection of human rights during wartime, offering an innovative approach to metaverse integration.

Theoretical Framework

1. Artificial Intelligence and the Transformation of Approaches to Border Security in Ukraine

Under current conditions of intensified global turbulence and the rise of complex transnational threats, ensuring border and state security occupies a special place within the framework of public policy - especially for countries located in zones of geopolitical tension. Ukraine, as a nation that has essentially become a stronghold of European security, faces extensive challenges: armed aggression from an external adversary, the spread of hybrid threats, increased illegal migration, widespread smuggling, human trafficking, and other manifestations of transnational crime.

In such circumstances, the urgent need arises to modernize border management models, integrate technology-driven AI solutions, and reassess border protection strategies with respect to human rights and associated guarantees.

A key guiding principle in this process is the ethical transformation of the civil and law enforcement service. In the modern security discourse, the principles of integrity and ethical conduct of public officials -

particularly border and law enforcement personnel - take on paramount importance. The concept of "integrity" is treated not only as a moral quality but as a foundational principle of public administration that ensures transparency, impartiality, political neutrality, and conscientious execution of duties. This approach is grounded in the provisions of the Constitution of Ukraine, anti-corruption legislation, and the principles of service to the people and society [15].

According to the Law of Ukraine "On the State Border," securing the border is an element of the overall national security system, implemented through collaboration between military units, border guards, and law enforcement agencies. This process involves not only the physical protection of boundaries but also a wide spectrum of measures - ranging from diplomatic and political to intelligence, technical, and environmental efforts [16]. In this context, the significance of artificial intelligence grows, offering not just automation but deep analytics and strategic threat forecasting.

Scholarly research by Ukrainian legal experts - including Averianov V. B., Bandurka O. M., Bytiak Yu. P., Halunko V. V., Kalyuzhnyi R. A., Kalpakov V. K., Muzychuk O. M., Nikitenko O. I., Lipkan V. A., Kostenko O. V., Predmestnikov O. H., Tatsiiy V. Ya., Shemshuchenko Yu. S., and others - has long addressed the integration of AI in the security sector, highlighting the need for legislative frameworks and ethical boundaries. Administrative and legal regulation, especially regarding the preparation of international agreements on cooperation with neighboring countries, is also influenced by digitalization trends and the adoption of intelligent technologies within the national defense system.

Given the digital transformation of the world and rapid IT development, the state border is now viewed not only as a physical line but as a complex digital and security system requiring new approaches to protecting sovereignty, territorial integrity, and ensuring economic and informational security through Ukrainian law enforcement agencies. The use of AI in this context enables more efficient threat detection and adaptation to cyber challenges - particularly in conditions of hybrid warfare. Intelligent video analytics systems, automated risk assessment algorithms, biometric scanners, and computer vision are already employed by modern border services, including joint projects with Frontex, where Ukraine actively cooperates in combating illegal migration and human trafficking.

Under international law, a key principle for stable interstate relations is the inviolability of state borders. States are obliged to refrain from any actions that might undermine another country's territorial integrity. Peaceful coexistence, respect for sovereignty, and compliance with international obligations are the foundation of a legal order that supports global security. Any changes to borders must occur exclusively through mutual consent, within a framework of dialogue and in accordance with international law [8].

However, modern realities reveal the intensification of transnational crime, particularly in border regions. These areas have long ceased to be mere lines dividing states - they have become hotspots of criminal activity, where illegal migration, smuggling, and trafficking in weapons, drugs, and people flourish.

In this new security context, artificial intelligence begins to play a special role. With its ability to process vast volumes of data, integrate information from diverse sources, and identify patterns, AI becomes a powerful tool for forecasting, anomaly detection, and operational intervention. This enables not only the documentation of violations but also their early prevention - through behavioral analysis, identification of risky routes, and predictive scenarios.

It is important to emphasize that the potential of AI goes far beyond physical border protection. Its strategic use in safeguarding digital space is particularly relevant in conditions of hybrid warfare and cyberattacks. National sovereignty today is defined not only by the ability to control territory but also by effectiveness in protecting information infrastructure and digital independence.

Border security in the 21st century represents a synergy of physical, legal, and technological tools operating within a unified system of prevention and response. Respect for the state border entails not only respect for territorial integrity but also for the rule of law, digital ethics, and responsible use of innovative technologies such as AI.

Technological progress enables a rethinking of the logic of border control itself. Whereas in the past the main task was to respond to offenses already committed, today the focus shifts toward managing risks before they materialize. AI-driven systems make it possible to assess the likelihood of dangerous scenarios, analyze behavioral anomalies, and automatically identify atypical routes, transactions, and actions that may signal preparation for a violation. This supports proactive, economically efficient, and highly precise control.

A particularly relevant concept in this context is that proposed by American scholar G. Albanis, who argues that the cessation of criminal offenses is impossible without addressing the root causes - the socio-

economic demand for goods and services controlled by the criminal world [18]. Border territories, often left in the shadows of state policy, become gray zones where such challenges are most concentrated.

Artificial intelligence in this case not only facilitates responsive action but also enables the identification of socio-economic trends that contribute to criminal activity. Demand analysis, assessment of the social climate, and the identification of so-called "flash points" - all these capabilities allow not only for the containment of crime but also for addressing its underlying causes.

In the era of rapid technological change and global challenges, a new security architecture is emerging - more flexible, dynamic, and adaptive. It is founded not so much on intuitive responses to events, but rather on a profound understanding of systemic interconnections and the forecasting of threats. Within this context, artificial intelligence (AI) serves not merely as a technical tool, but as a conceptual instrument of future security. Its integration with international law norms, the values of social responsibility, and the rule of law forms a new philosophy of security - responsible, digital, and transparent.

Intelligent systems based on machine learning algorithms, computer vision, and behavioral analytics are already capable of autonomously detecting suspicious actions at checkpoints, analyzing vehicle movements, recognizing faces, and processing video streams in real time. This allows for enhanced responsiveness and effective allocation of limited resources to the most critical border areas.

The implementation of AI in the border sector marks the transition to a new, intellectualized model of state control. It is not merely about modernizing individual elements, but about creating a comprehensive "Smart Border System," in which all components - from databases and video systems to analytical centers - operate in interaction based on a unified digital platform. In such a system, AI becomes not a supporting tool but a strategic center for decision-making.

For Ukraine, which is both a direct neighbor of the European Union and a country experiencing armed aggression, the deployment of AI in the border sector is not just desirable but vitally necessary. The use of intelligent technologies in public administration helps to compensate for the shortage of human and technical resources, especially during martial law, when every control tool acquires strategic importance.

At the same time, active digitalization and the use of intelligent systems present new demands for legal regulation. Like any high-tech system, AI entails risks - including violations of human rights, dishonest data collection, and the danger of discriminatory decisions made by algorithms without sufficient human oversight. That is why the transformation of border policy must be accompanied by a deep legal reform that establishes clear frameworks for AI use and guarantees transparency, accountability, and effective protection of citizens' fundamental rights.

These issues are directly intertwined with the need for a profound renewal of Ukraine's law enforcement system. Currently, the national legal landscape reveals significant ambiguity regarding the definition of "law enforcement agencies." Depending on interpretation, Ukraine has between 17 and 80 agencies performing law enforcement or legal enforcement functions [19]. Such ambiguity complicates the development of coherent security policy, including border security.

At the same time, the Law of Ukraine "On State Protection of Employees of the Judiciary and Law Enforcement Agencies" clearly outlines the scope of agencies holding this status. These include the Prosecutor's Office, the National Police, the Security Service, the Military Law Enforcement Service within the Armed Forces of Ukraine, the National Anti-Corruption Bureau of Ukraine, border protection bodies, the Bureau of Economic Security of Ukraine, penal enforcement agencies, pre-trial detention centers, financial control bodies, fisheries protection, state forestry protection, and other agencies performing legal enforcement or law enforcement functions. For the effective functioning of a digital security system in which AI acts as a central element, clear legal structuring and coordination among these institutions are required. Only with transparent regulation of powers and division of responsibility can modern tools, including AI, become an effective pillar of the national security system.

In an environment of legal pluralism and blurred functional boundaries between agencies that perform law enforcement and security functions, Ukraine's state security system faces multiple challenges. One key issue is the internal contradiction in defining the powers and competencies of various institutions. This, in turn, leads to functional ambiguity, which hinders the development of a comprehensive, coordinated policy in the field of security in general and border security in particular.

In such circumstances, the need for deep legal reform becomes especially relevant - a reform that would create a clear and transparent system for delineating responsibilities among state security entities. This reform must not only streamline the existing regulatory framework, but also establish the prerequisites for effectively integrating modern digital technologies, particularly artificial intelligence. Clearly defined authorities,

responsibilities, and mechanisms for inter-agency cooperation will form the basis for harmonious functioning of border protection systems, cyber security assurance, and digital sovereignty.

Ukraine today is in a unique position - not only does it possess the political will for change, but it also has a strategic drive to implement innovative approaches to security. Artificial intelligence, integrated into the legal field with adherence to international standards of human rights protection, can become not merely a technical solution, but a core component of a new, flexible, and effective model of state security.

This model involves not just instrumental use of technology, but the implementation of a culture of digital responsibility, legal regulation, and ethical oversight [20]. Ukraine has every opportunity to become a model for Central and Eastern European countries, where digital transformation in the security sphere is combined with the rule of law, transparency of state decisions, and respect for human dignity.

2. Artificial Intelligence as a Tool for Countering Border-Related Criminal Offenses

In today's world, where global security is constantly under threat due to instability, conflict, migration crises, and rapid digitalization, border crime emerges as one of the most dangerous forms of transnational illegal activity. Its nature is defined by exceptional flexibility, multidirectionality, and a high degree of adaptability to changes in political, economic, and social contexts. This refers not only to its classic manifestations - such as illegal migration, smuggling of tobacco, alcohol or fuel, and drug trafficking - but also to much more sophisticated schemes that involve trafficking in firearms, financial fraud, money laundering, and cybercrime, which is especially perilous in the context of contemporary hybrid warfare.

For Ukraine, which serves as the external shield of the European Union while simultaneously facing large-scale armed aggression, the threats of border-related crime possess not only criminal but also distinctly national dimensions. Regions adjacent to temporarily occupied territories or functioning as transit routes for the illegal movement of people and goods are transforming into hubs of criminal activity, infused with elements of political pressure, informational manipulation, and economic destabilization. Traditional tools for combating such threats - including patrolling, document checks, and intelligence operations - are increasingly proving ineffective, particularly against the backdrop of evolving threats and resource deficits.

One of the most urgent and strategic tasks confronting Ukraine's law enforcement system is the transformation of its existing crime prevention model toward high-tech approaches based on innovative digital solutions. At the core of this shift lies the use of artificial intelligence (AI) technologies, which can not only automate routine operations but also significantly improve the analytical capacity of law enforcement agencies. In particular, AI enables efficient processing and analysis of massive datasets - so-called Big Data - collected from various sources including information systems, social networks, financial transactions, and other digital traces. These capabilities unlock a unique opportunity to forecast criminal activity even at its early stages.

AI systems can detect complex patterns, uncover hidden relationships between subjects and objects of criminal acts, and deliver timely analytics that allow law enforcement agencies to make fast and accurate decisions. The implementation of such technologies creates the conditions for a shift toward anticipatory response, where the focus moves from investigating crimes after they occur to active preventative action designed to avert violations before they happen. This approach not only enhances public safety, but also optimizes the allocation of law enforcement resources, reducing costs associated with investigations and remediation of criminal consequences.

At the same time, it is critical to recognize that border-related crime is not limited to a collection of isolated criminal episodes, but constitutes a complex socio-political phenomenon with a multidimensional structure. It encompasses struggles for control over key logistical routes, the division of influence among criminal groups, and the creation of shadow power hierarchies outside official jurisdiction. A distinctive feature of such a criminal ecosystem is the use of mechanisms akin to "arbitration courts," where conflicts and disputes between criminal clans are resolved by so-called "authorities" or "criminal leaders," who are recognized and legitimized within the criminal milieu. These parallel institutions maintain a certain "order" within the criminal world, while simultaneously generating serious public concern and acting as a catalyst for intensified efforts by state law enforcement agencies aimed at suppressing illicit influence and restoring the rule of law [21].

Within this complex and multi-layered political and administrative landscape, the role of artificial intelligence transcends traditional analytics and acquires strategic importance. Thanks to its capacity for in-depth analysis of information arrays, AI enables the identification of subtle but significant long-term trends in the operations of criminal organizations, establishes intricate interconnections between illicit flows of goods, finances, and people, and forecasts potential escalation of conflicts in border regions. Through risk scenario modeling, AI-

based systems assist law enforcement agencies in more effectively planning the deployment of forces and resources, optimizing operational measures, and improving the agility of response to emerging challenges.

In today's security environment, shaped by global instability, hybrid threats, and transnational crime, improving the mechanisms of administrative and legal support for law enforcement activities becomes critically important. This encompasses guaranteeing civil rights and freedoms, combating corruption and smuggling, addressing crimes in the sphere of migration, drug trafficking, and international terrorism. In the context of reforming Ukrainian society and state institutions, particular emphasis is placed on transforming the legal system to ensure constitutional foundations, the principle of rule of law, and legality in the operations of security agencies - especially in border regions.

Law enforcement agencies ensure internal stability in frontier areas and must respond to a wide array of threats - ranging from energy to environmental, from illegal resource extraction to transportation infrastructure protection. The effectiveness of this process depends on interdisciplinary cooperation and the involvement of key branches of public law: administrative, constitutional, informational, economic, customs, and environmental. Each of these forms the legal foundation of a contemporary model of national security.

Administrative law as a distinct legal branch has deep historical roots dating back to the 18th century, and has always been closely tied to the exercise of public authority, organization of civil service, and interaction between government and citizens [22]. In present conditions, administrative-law mechanisms serve as tools for implementing reforms aimed at strengthening state control and affirming the principle of legal certainty. As highlighted in the "Concept of Administrative Law Reform in Ukraine," the primary goal of these changes is to ensure humane and efficient government operation in accordance with European legal standards [23].

Within this context, artificial intelligence plays a pivotal role in expanding the capabilities of border security. Machine learning algorithms are not only able to analyze historical data and identify behavioral patterns, but also forecast criminal violations, enabling law enforcement agencies to take preemptive action. This provides a strategic advantage in resource management - allowing for their rapid allocation to the most vulnerable areas.

One of the most technologically promising domains of AI application is automated video analytics. Unlike traditional models where operators manually review footage, intelligent systems can detect suspicious behavior, flag anomalies, and recognize faces and license plates in real time. Computer vision, as a core component of AI, significantly enhances law enforcement's ability not only to respond to crimes but to prevent them.

This is especially relevant for Ukraine, which faces external armed aggression while fulfilling the function of the EU's external border. Enhancing border security through intelligent technologies not only supports internal stability but also reinforces Ukraine's standing as a reliable partner within the European security architecture. The use of AI in border control must evolve into more than a technical solution - it should be an element of an integrated legal and administrative strategy focused on effectiveness, human rights compliance, and legal transparency.

Ensuring effective border security entails far more than simply monitoring the movement of individuals and goods across national boundaries. Under current conditions, it is a multifaceted system directly tied to national sovereignty, territorial integrity, internal stability, and the overall system of public order protection. As emphasized in [24], border security serves as a criterion of a state's ability to exercise public authority and maintain law and order - not only at the local level, but in the broader European context, where the security of one nation is inextricably linked to that of its neighbors.

In this context, the role of artificial intelligence (AI), particularly in document verification, becomes critically important. Through technologies such as computer vision, text recognition, and biometric identification, modern border systems are capable of instantly checking documents for authenticity, cross-referencing them against search databases, analyzing structural anomalies, and detecting falsifications. This significantly reduces risks associated with human error and boosts both the precision and speed of decision-making in border control processes.

Another critically important area of AI application is in analytical systems. With its ability to process large volumes of data from diverse sources - satellite imagery, customs databases, police registries - artificial intelligence enables the modeling of smuggling routes, construction of profiles for potentially dangerous individuals, identification of recurring violation patterns, and development of predictive models. This allows a shift in emphasis from reacting to crimes after they've occurred to proactive prevention and strategic risk management.

This approach becomes particularly relevant in the context of the digitalization of criminal activity. Modern cross-border offenses increasingly move into cyberspace, where coordination, financing, trade in personal data, and the deployment of malicious campaigns take place. In such cases, AI serves not only as a "border guard" but also

as a cyber-operator - identifying cyber threats, detecting attempts of unauthorized access to government information systems, and analyzing financial transactions potentially tied to organized crime or terrorist networks. Deep learning algorithms can reveal connections between cyber incidents and physical movements of violators across national borders, contributing to a unified framework of national security.

Another important aspect is the international integration of Ukraine's border policy, particularly through partnerships with Interpol, Europol, Frontex, and the EU's border law enforcement agencies. In this context, the use of AI enables Ukraine to align its security mechanisms with advanced European standards of digital monitoring, data verification, information exchange, and criminal analysis. This forms the foundation for Ukraine's full-fledged participation in the creation of a common European security space, where data and algorithms safeguard borders.

At the same time, the rapid implementation of intelligent technologies necessitates swift response from legal and ethical systems. Protection of personal data, ensuring algorithmic transparency, and the introduction of independent external oversight - all these are necessary components of the legitimate use of AI. It's about achieving a balance between security and human rights, especially in border regions that often become zones of heightened state control.

3. International experience in legal regulation of AI usage in the context of national security within Ukraine's border regions

Global experience in the consolidation of European values, legal standards, and human rights protection serves as a key factor in shaping integration policy. In light of current geopolitical transformations and threats - notably the armed aggression of the Russian Federation against Ukraine - a comprehensive analysis of the political, legal, and security dimensions of the Association Agreement between Ukraine and the European Union becomes critically important. Within the Eurointegration framework, Ukraine commits to upholding the core principles of democracy, rule of law, and respect for human rights, including minority rights, and actively implementing relevant European norms in its national legislation.

These processes extend not only to humanitarian and human rights domains but also directly relate to the strategic sphere of national security, including the protection of sovereignty, territorial integrity, national borders, internal order, and anti-corruption efforts. Responsibility for ensuring these functions lies with the military formations and law enforcement agencies, whose activities are regulated by special laws in accordance with the Constitution of Ukraine. In this context, aligning domestic legislation with EU standards gains particular importance - especially regarding the prevention of internal threats, countering hybrid challenges, and refining anti-corruption mechanisms.

In the 21st century, EU member states face a range of complex and interconnected security challenges: escalating hybrid threats, waves of illegal migration, cybercrime, terrorism, transnational organized crime, and technological asymmetry in the security sector. These challenges require not only strengthened institutional capacity in security bodies but also a fundamental rethinking of security policies. That is why EU states are investing in innovative technologies - particularly the deployment of artificial intelligence (AI) as an effective tool to respond to complex challenges. AI applications increasingly permeate border control, critical infrastructure protection, threat detection, and cybercrime combat.

At the same time, special attention in Europe is devoted to the legal regulation of AI systems. This covers not only technical aspects of algorithmic operation but also fundamental issues such as human rights, ethics, and transparency. In this context, a major milestone was the adoption in 2024 of the landmark AI Act - the world's first comprehensive legal framework governing AI usage. The Act enshrines a risk-based approach: all AI systems are classified according to their potential threat levels - from minimal to unacceptable. For example, systems used in security, law enforcement, or border management are designated as high-risk, while citizen social scoring systems are prohibited.

The AI Act also establishes strict requirements for AI developers and providers: they are obliged to follow principles of transparency, explainability of algorithms, human oversight of automated decision-making, and protection of personal data. Thus, legal regulation becomes a cornerstone in harmonizing technological development with the core values of the European Union.

Beyond regulatory frameworks, the practical implementation of AI in the security domain is supported by ethical and technical standards jointly developed by the European Commission, ENISA, Frontex, academic institutions, and private-sector stakeholders. This coordination facilitates the formation of an integrated EU security space, where technologies operate according to the principles of openness, ethics, and efficiency. AI

standards not only establish technical protocols but also align them with EU law, universal human rights, and member states' national interests [32] .

One of the most successful examples of technological integration into border policy is the creation of the "Smart Borders" system, coordinated by Frontex. This system includes a range of innovative solutions: automated biometric verification, identity confirmation via artificial vision, and behavioral analysis of travelers to identify potential risks. For instance, deep learning-based systems can not only recognize faces but also predict risks based on abnormal behavioral patterns. This enables an effective early warning system for potential threats - particularly relevant amid rising illegal migration and terrorist risks.

In EU countries such as Germany, France, and Italy, AI implementation in border management is systematic and comprehensive. In Germany, autonomous drones with advanced sensors and infrared cameras are actively used to monitor border areas in real time. Image recognition algorithms allow for rapid identification of suspicious activity. In France, given the high passenger flow, AI systems are deployed in airports and major railway stations to perform traveler identification without border guards - significantly speeding up document checks and reducing misidentification risks. In Italy - with its Mediterranean coastline and proximity to key migration routes from Africa - AI is used to create predictive models: algorithms analyze migrant flows, weather conditions, and political developments in North African countries, enabling authorities to preemptively plan crisis responses and ease the burden on border services.

Overall, the European approach to AI usage in the security domain showcases a model that combines technological advancement with democratic values and human rights. Such a framework can and should serve as a guiding benchmark for Ukraine. As it moves along the path of European integration, Ukraine must consider not only the EU's technical achievements but also its legal and ethical standards amid ongoing challenges posed by the aggressor. At the same time, the experience of EU member states can be adapted to Ukrainian realities - taking into account the specific conditions of martial law, hybrid threats, and the need to effectively safeguard citizens' rights and freedoms in a conflict setting.

However, technological progress alone cannot justify the weakening of democratic and legal oversight over the use of artificial intelligence. On the contrary, European experience confirms that the development and spread of powerful technologies must be accompanied by stricter standards of ethical responsibility and legal accountability. A key component of this system is the principle of algorithmic transparency: citizens have the right to receive clear explanations regarding decisions made by automated systems, as well as the ability to contest such decisions through legally established procedures. Many EU countries have specialized ethics commissions and oversight councils that conduct expert assessments on the appropriateness of deploying AI systems - particularly in sensitive areas where the risk of human rights violations exists. These areas include automated migrant filtering, biometric data processing, and intelligent video surveillance in public spaces - all of which require focused regulation and oversight.

In today's digital world, where technologies permeate every aspect of life, active involvement of civil society in shaping AI-related policies takes on special importance. In the EU, human rights organizations - such as Access Now, European Digital Rights, Amnesty International, and others - play a significant role in consultations and public oversight of innovative technology deployment. Their work aims to maintain the balance between state security needs and the protection of fundamental rights and freedoms. One of the most pressing concerns is the widespread use of biometric systems and intelligent video surveillance in public areas, often without the informed consent of the individuals being monitored.

It was precisely under public pressure that strict limitations were introduced in European legislation - including the AI Act - on the use of certain types of artificial intelligence in open public spaces. The ban applies to systems that may infringe on privacy and freedom rights, except for justified cases defined by law. These exceptions include, among others, preventive measures against terrorist attacks and operational search activities related to individuals suspected of serious crimes. This points to the emergence of a new security concept in Europe - one in which technology serves society, not as a tool of control by automated systems.

In this context, it is especially important for Ukraine - which is steadily progressing toward full EU membership - not only to adopt the latest artificial intelligence technologies in its law enforcement, defense, and border security structures, but also to systematically adapt European approaches to regulating the ethical, legal, and social aspects of their use. This means going beyond merely importing technical solutions - instead initiating a comprehensive transformation of the regulatory framework to ensure transparency and accountability in digital technology application, establishing independent public oversight institutions, and actively participating in joint international initiatives for shaping the digital security space.

Already today, Ukrainian border services demonstrate a high level of readiness for integration into European security mechanisms. Their cooperation with Frontex - the European Border and Coast Guard Agency - stands as a vivid example of a commitment to deepening partnerships based on modern technological solutions. Within these projects, AI-based systems are actively employed to efficiently detect illegal migration routes, counter human trafficking, analyze migration flows, and rapidly respond to potential threats.

It is essential to highlight that this cooperation goes far beyond mere technical data exchange - it entails the implementation of a new paradigm in law enforcement and border management, one that combines preventive security measures with the highest attention to human rights compliance. The intellectualization of Ukraine's law enforcement system through AI is not just a tool to enhance effectiveness - it is also an expression of responsibility, transparency, and alignment with the values of the European legal space.

Materials and Methods

The study was carried out using a comprehensive methodological approach focused on the analysis of legal regulation regarding the use of artificial intelligence (AI) in ensuring national security within Ukraine's border areas, with an emphasis on the potential of the metaverse. The methodology combines comparative legal analysis, systems analysis, review of international experience, and evaluation of AI's technological capabilities. This approach enabled the assessment of the current legislative framework, identification of regulatory gaps, examination of international practices, and the development of recommendations for improving the regulatory base in accordance with the principles of rule of law and ethical use of technology [24].

Research Sources

The foundation of the research consisted of normative legal acts of Ukraine regulating border security and law enforcement activities. In particular, the Constitution of Ukraine [1], the Law of Ukraine "On the State Border of Ukraine" [16], and the Law of Ukraine "On the State Border Guard Service of Ukraine" [31] were analyzed. Additionally, the Concept of Administrative Law Reform in Ukraine [23] and the AI Development Concept in Ukraine until 2030 [4] were reviewed, which outline strategic directions for implementing innovative technologies.

To analyze international experience, normative documents of the European Union [10] were used, including the EU AI Act of 2024, which sets standards for ethical AI use, and reports from the European Border and Coast Guard Agency (Frontex) [12] regarding the use of AI in border management.

The scholarly literature reviewed included works on constitutional, administrative, information, and service law [15]; internal security [3, 28]; combating transborder crime [8, 17, 18, 27]; and constitutional guarantees for the protection of human rights [19, 29]. Special attention was given to works dedicated to the professional activities of the Border Guard Service and its legal legitimacy in protecting Ukraine's sovereignty and territorial integrity [14, 26].

Research Methods

The primary research method used was comparative legal analysis, applied to compare Ukrainian legislation with international standards regulating AI. This method enabled an assessment of the compliance of the Laws of Ukraine "On the State Border of Ukraine" and "On the State Border Guard Service of Ukraine" with current requirements for AI implementation, as well as the identification of gaps in legal regulation [16, 31]. Specifically, it was established that existing legislation does not contain provisions regulating the use of AI for automating border control, identity recognition, or threat forecasting [3].

Systems analysis was employed to study the interrelationship between AI technologies, border security, and the metaverse as a platform for modeling security scenarios. This method helped determine how AI can optimize document verification processes, analysis of video streams from cameras and drones, as well as risk forecasting, such as smuggling or illegal border crossings [22].

The systems approach also allowed for an assessment of the potential integration of AI with the metaverse to create virtual simulations that enhance the effectiveness of border guard training [14].

The study of international experience was conducted through analysis of practices in European Union countries, the USA, and NATO. In particular, it examined AI usage in the USA for monitoring the border with Mexico, where object recognition and behavior analysis algorithms are applied [17], as well as AI usage in the EU for migration flow forecasting within Frontex operations [12]. Ethical aspects of AI usage were evaluated based on INTERPOL's Code of Ethics, which emphasizes transparency and the protection of human rights, notably the right to privacy [24].

Analysis of the Potential of the Metaverse

A separate research direction involved examining the possibilities of integrating AI with the metaverse for border security needs. The metaverse is considered a virtual environment that allows for modeling border operations, training personnel, and testing response scenarios to threats such as smuggling, illegal crossings, or hybrid attacks. A qualitative analysis method was applied to evaluate scholarly publications and practical cases involving virtual platforms in the security domain. For example, virtual simulations allow for real-world situations to be recreated in a controlled setting, enhancing border guards' readiness to respond to complex challenges without exposing them to real-world risks.

To assess the ethical and legal aspects of AI use in the metaverse, principles of rule of law and human rights protection presented in academic literature were analyzed [19, 29]. This analysis enabled the formulation of recommendations for establishing a legal framework that regulates AI use in border security while considering ethical standards.

Research Organization

The research was conducted in several stages. In the first stage, normative legal acts, scholarly sources, and reports from international organizations were collected and systematized. In the second stage, a comparative analysis of Ukrainian and international legislation was carried out. In the third stage, the technological capabilities of AI - particularly in the metaverse context - were evaluated and recommendations were developed. All data were processed using open sources, including the databases of the Verkhovna Rada of Ukraine, official EU websites, and academic journals [19, 29].

Results

The conducted study yielded findings concerning the current state of legal regulation regarding the use of artificial intelligence (AI) in Ukraine's border security, the possibilities for its application, and the potential for integration with the metaverse. The analysis, based on comparative legal analysis, systems modeling, and review of international experience, identified key gaps in legislation and evaluated the prospects of AI to enhance border control effectiveness [3, 22].

Analysis of Ukrainian Legislation

The analysis of Ukraine's regulatory framework revealed that current legislation lacks specific norms regulating AI use in the border security domain. The Law of Ukraine "On the State Border of Ukraine" [16] defines core principles for protecting the state border but does not contain provisions regarding the deployment of modern technologies such as AI. Similarly, the Law of Ukraine "On the State Border Guard Service of Ukraine" [31] governs the activities of the Border Guard Service but does not cover the use of AI-based automated systems for identity verification, data analysis, or threat forecasting.

The AI Development Concept in Ukraine until 2030, approved by the Cabinet of Ministers, focuses primarily on economic and technological aspects of AI development - such as supporting innovation and digitalization - but does not contain specific provisions regarding its use in the security sector [4]. This creates legal uncertainty, complicating AI deployment in the border domain and increasing risks of human rights violations, notably the right to privacy [19, 24].

The analysis established that the absence of regulatory norms for AI in border security leads to several problems. First, there are no clear standards for ethical AI use, which could result in abuse of technology - such as excessive surveillance or unjustified profiling. Second, the lack of legal provisions hinders the integration of AI systems into the operations of the State Border Guard Service of Ukraine, reducing their effectiveness [28]. Third, the absence of legislative mechanisms for interagency coordination slows the implementation of comprehensive AI systems for border monitoring [26].

Potential Applications of AI in Border Security

Research has revealed significant potential for AI to enhance the efficiency of border control in Ukraine. Specifically, AI can be used for:

- **Automated Document Verification**: AI algorithms enable rapid processing of passport data, detection of forged documents, and comparison with databases [8].
- **Person Identification**: Facial recognition and biometric identification systems can be used to verify individuals at checkpoints, improving the speed and accuracy of control [5].

- **Video Stream Analysis**: AI systems integrated with cameras and drones are capable of detecting suspicious behavior or objects in real time [3].
- **Threat Prediction**: Machine learning models allow for analysis of data on migration flows, smuggling, or hybrid threats, contributing to preventive measures [22].

The application of AI in the border sector can significantly reduce the burden on personnel, improve the accuracy of violation detection, and shorten response times to threats. For example, AI systems can process large volumes of data from sensors and cameras, enabling prompt responses to illegal border crossings or smuggling attempts [14].

International Experience in AI Application

Analysis of international experience shows that the European Union, the United States, and NATO countries are actively deploying AI in border security. In the U.S., AI is used to monitor the border with Mexico, where object recognition and behavior analysis algorithms help identify illegal crossings and smuggling. In the European Union, Frontex utilizes AI to forecast migration flows and assess risks, allowing for optimized resource allocation at borders. The EU AI Act of 2024 establishes clear requirements for transparency, safety, and ethical standards of AI systems used in security domains, including data protection and the prevention of discrimination.

In NATO countries, AI is employed to simulate security scenarios and train personnel, particularly through virtual platforms integrated with the metaverse. For instance, virtual simulations enable the recreation of hybrid threat scenarios, such as cyberattacks or sabotage, in a controlled environment. These practices demonstrate AI's effectiveness in enhancing the preparedness of border services to face complex challenges.

Table 1. Comparison of AI Regulation in Ukraine and the EU

Aspect	Ukraine	European Union
Legal Framework	Fragmented, no specific AI regulations	Comprehensive AI Act (2024) with risk-based approach
Transparency	Limited transparency in AI deployment	Mandates explainable algorithms and public reporting
Human Oversight	Minimal oversight, ad-hoc implementation	Requires human-in-the-loop for high-risk systems
Data Protection	Weak enforcement of data privacy laws	Strict compliance with GDPR
Metaverse Integration	No regulations for virtual simulations	Emerging standards for virtual platforms

Potential for AI Integration with the Metaverse

One of the key outcomes of the study is the assessment of the potential for integrating AI with the metaverse for border security purposes. The metaverse, as a virtual environment, allows for the creation of simulations of border operations that replicate real scenarios, such as the detection of smuggling, illegal border crossings, or responses to hybrid threats. AI systems integrated with the metaverse can:

- Model offender behavior and predict their actions based on data from previous incidents
- Train border guards in a virtual environment, reducing the cost of practical training and personnel risk [26]
- Test AI systems in simulated conditions before deployment in the real world

Analysis revealed that using the metaverse in combination with AI enables the creation of interactive training platforms where border guards can practice responding to complex situations such as mass migration flows or terrorist threats. For instance, virtual simulations can replicate checkpoints with realistic scenarios, improving professional preparedness.

However, the absence of legal regulations governing the use of AI in the metaverse in Ukraine presents additional challenges. Specifically, there are no norms that define data security standards, ethical use of simulations, or the protection of individuals whose data is used in virtual environments. This highlights the need to develop specialized legislation that considers the unique features of the metaverse.

Discussion

The results presented in the previous section indicate a significant potential of artificial intelligence (AI) in ensuring Ukraine's border security, as well as substantial gaps in existing legislation that hinder its effective implementation. This section interprets the results by comparing them with international standards, analyzing opportunities and risks of AI use - particularly in the context of the metaverse - and proposes recommendations for improving Ukraine's legal framework.

Gaps in Ukrainian Legislation

Analysis of Ukrainian law revealed that the Laws of Ukraine "On the State Border of Ukraine" and "On the State Border Guard Service of Ukraine" lack provisions regulating AI use in the border domain. This aligns with the findings of [11], which noted that Ukraine's regulatory framework is lagging behind technological advancements in the security field. Compared to international standards - specifically the EU AI Act 2024 - Ukrainian legislation does not establish requirements for transparency, safety, and ethical standards in AI systems, which creates risks for human rights violations, especially the right to privacy. For example, the EU AI Act mandates a clear classification of AI systems based on risk levels, whereas Ukraine lacks such standards, complicating the deployment of AI at border checkpoints or monitoring systems.

The absence of specialized norms in Ukrainian legislation also impedes interagency coordination, which is critical for comprehensive AI use in border security. International experience, particularly Frontex's practices, shows that successful AI implementation requires interagency cooperation and clear legal frameworks. In this context, study findings emphasize the need to develop a separate legislative act or amend current laws to regulate AI use in the border domain.

The Importance of AI for Border Security

Study findings confirm the significant potential of AI in enhancing border control efficiency, which aligns with international research. Automation of document verification, biometric identification of individuals, and analysis of video streams from cameras and drones can significantly reduce data processing times and increase violation detection accuracy. For example, in the U.S., AI algorithms applied at the Mexico border can detect suspicious behavior in real time, reducing strain on border guards. In Ukraine, similar technologies could be used to combat smuggling and illegal border crossings, particularly amid hybrid threats.

Threat prediction using machine learning models, as highlighted in the results, is another important aspect. It allows the border service to proactively plan measures to prevent migration crises or cross-border crime. However, as noted in [24], implementation of such technologies must be accompanied by clear ethical standards to avoid human rights violations, such as unjust profiling or excessive surveillance.

Integration of AI with the Metaverse

Among the most promising findings of the study is the potential of integrating AI with the metaverse to simulate border scenarios. Virtual simulations, as the analysis showed, allow for recreating real situations such as illegal border crossings or smuggling in a controlled environment, reducing training costs and personnel risks. These findings align with NATO countries' international experience, where the metaverse is used for security force training, including modeling hybrid threats.

Compared to traditional training methods, the metaverse in combination with AI offers unique opportunities to create interactive platforms where border guards can practice responding to complex scenarios such as terrorist attacks or mass migration flows. For example, virtual checkpoints can simulate offender behavior, allowing AI to predict their actions based on previous data. However, as the results show, use of the metaverse in Ukraine is restrained by the lack of legal norms regulating data security and ethical aspects of such simulations.

Comparisons with international experience, particularly INTERPOL's Code of Ethics, emphasize the need to develop standards for AI use in the metaverse to ensure data protection and prevent abuse (Code of Ethics for INTERPOL Officials, n.d.). For instance, in the EU, AI systems integrated with virtual platforms are subject to strict transparency and safety controls, which could serve as a model for Ukraine.

Risks and Challenges

Study results point to several risks associated with AI use in border security. First, the lack of legal regulation may lead to human rights violations, particularly through unjustified use of biometric data or profiling algorithms [24]. Second, Ukraine's technical infrastructure, compared to EU or U.S. standards,

complicates the implementation of AI systems at borders. Third, integrating AI with the metaverse requires substantial investment in digital technologies and personnel training, which is challenging for Ukraine under resource constraints.

These risks are consistent with international research emphasizing the need for balance between technological innovation and ethical standards. For example, in the U.S., AI implementation is accompanied by strict data protection rules, while in Ukraine such mechanisms are absent, increasing the likelihood of abuse.

Recommendations and Outlook

Based on the study findings, several recommendations can be made to improve legal regulation of AI in Ukraine's border security:

1. Develop a separate legal act to regulate AI use, including standards for ethics, transparency, and data protection, based on the EU AI Act 2024
2. Create an interagency coordination group to integrate AI into border service operations, which will optimize resources and increase effectiveness
3. For metaverse use, develop national standards for virtual simulations that account for data security and human rights

Future research may focus on developing specific AI models for border security, evaluating their economic efficiency, and analyzing the impact of the metaverse on professional training of border guards. These areas will support Ukraine's integration into the European security space and enhance border control effectiveness.

Conclusions

This study undertook a theoretical analysis of a pressing issue - the development of a scientifically grounded concept for ensuring state security in the border regions of Ukraine. Particular attention was given to protecting the state border through law enforcement agencies, along with formulating recommendations and proposals for improving legal regulation of artificial intelligence (AI) use in the relevant field. It should be noted that the security of border territories is an integral component of Ukraine's national security. The collection of corresponding measures forms a comprehensive concept of internal and national security aimed at countering external and internal threats.

In the context of legal reform and the formation of a national legal system capable of meeting current challenges, reference to the provisions of Ukraine's Legal Doctrine - as outlined in the fundamental five-volume edition edited by V. Ya. Tatsiy, O. D. Sviatytskyi, S. I. Maksymov, and others, with general editorial direction by O. V. Petryshyn - takes on particular relevance. This comprehensive approach contributes to the creation of a coherent legal framework for ensuring state security, encompassing both constitutional and administrative legal dimensions.

The primary goal of legally regulating the implementation of AI in the field of state security in Ukraine's border regions is to develop and implement a strategy for improving national legislation, particularly regarding the constitutional order and procedures for amending the Constitution of Ukraine. This process is key to establishing a regulatory framework that will allow the integration of innovative security technologies into Ukraine's border areas and legal system, while ensuring adherence to constitutional principles and guarantees of national security protection [19].

Through the course of the research, it was established that the administrative-legal foundations regulating the use of AI for border security in Ukraine remain fragmented and underdeveloped both in academic literature and in practice. This situation underscores the urgent need for in-depth analysis and the creation of comprehensive legal mechanisms capable of governing the integration of innovative digital technologies, particularly AI systems, into state security on the administrative level.

Special attention in this context must be given to the legal legitimation of law enforcement activities responsible for maintaining state security in Ukraine's border regions. Currently, the effective functioning of these bodies is directly linked to ongoing reform processes in law enforcement, which must respond to contemporary challenges such as cyberactivity, hybrid threats, and illegal migration. The application of AI in the border domain can significantly improve monitoring capabilities, threat detection, and coordination among law enforcement and governmental agencies.

Legitimation, as a process of public and international recognition of the legitimacy of government actions, gains particular importance in transitional societies undergoing political transformation or internal conflict. Implementing AI in law enforcement without adequate legal regulation may result in public distrust,

which would, in turn, affect the legitimacy and effectiveness of the functioning of relevant state institutions. Therefore, forming a regulatory framework for transparent and accountable use of AI in border service activities should become a priority in the state security policy [20].

Thus, the conclusions formed in this study affirm the need for further development and refinement of the legal foundations for AI use in national border security, contributing to the protection of Ukraine's sovereignty and territorial integrity, safeguarding its economic and informational security and public order, and supporting the defense of the state border as a vital function of the state.

REFERENCES

1. *Constitution of Ukraine. Scientific and Practical Commentary* / editorial board: V. Ya. Tatsiy (chairman), O. V. Petryshyn (executive secretary), Yu. H. Barabash et al.; National Academy of Legal Sciences of Ukraine. – 2nd edition, revised and expanded. – Kharkiv: Pravo, 2011. – 1128 p.
2. *Constitution of Ukraine*, June 28, 1996, No. 254k/96-VR // Bulletin of the Verkhovna Rada of Ukraine – 1996 – No. 30 – Article 141.
3. Nikitenko, O. I. *Internal Security in the Border Regions of Ukraine: Monograph*. – Khmelnytskyi: National Academy of the State Border Guard Service named after Bohdan Khmelnytskyi; Bila Tserkva: BNAU, 2020. – 370 p.
4. *Concept for the Development of Artificial Intelligence in Ukraine*, approved by the Cabinet of Ministers of Ukraine, December 2, 2020, No. 1556-r. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text (Accessed: July 23, 2025)
5. Ana Beduschi. *International Migration Governance in the Age of Artificial Intelligence*. Migration Studies, Vol. 9, Issue 3, September 2021, pp. 576–596. https://doi.org/10.1093/migration/mnaa003
6. Yan, Y., Borgesius, F.Z., Beckers, P., Brauer, E. *Automated Decision-Making and Artificial Intelligence at European Borders and Their Risks to Human Rights*. ArXiv, abs/2410.17278 (2024). https://doi.org/10.48550/arXiv.2410.17278
7. La Fors, K., Meissner, F. *Contesting Border Artificial Intelligence: Applying the Guidance-Ethics Approach as a Responsible Design Lens*. Data & Policy, Vol. 4, No. 3, 2022, p. e36. https://doi.org/10.1017/dap.2022.28
8. Lyra, M.S., Damásio, B., Pinheiro, F.L., et al. *Fraud, Corruption, and Collusion in Public Procurement Activities: A Systematic Literature Review on Data-Driven Methods*. Applied Network Science, Vol. 7, 83 (2022). https://doi.org/10.1007/s41109-022-00523-6
9. Frontex. (2023). *Smart Borders: Bringing Frontex and Customs Closer Together*. https://www.frontex.europa.eu/media-centre/news/news-release/smart-borders-bringing-frontex-and-customs-closer-together-AzessI
10. European Commission. (2024). *EU AI Act: Regulation on Artificial Intelligence (Regulation (EU) 2024/...)*. https://eur-lex.europa.eu/eli/reg/2024/ (Accessed: July 23, 2025)
11. Buolamwini, J., Gebru, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency, pp. 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html
12. Frontex. (2023). *Smart Borders Initiative: Annual Report*. https://frontex.europa.eu/innovation/announcements/new-research-study-on-emerging-training-technologies-for-the-european-border-and-coast-guard-concludes-uBKS6Z
13. Lifelo, Z., Ding, J., Ning, H., Qurat-Ul-Ain, Dhelim, S. (2024). *Artificial Intelligence-Enabled Metaverse for Sustainable Smart Cities: Technologies, Applications, Challenges, and Future Directions*. Electronics, 13(24), 4874. https://doi.org/10.3390/electronics13244874
14. Nikitenko, O. I., Zhuravel, I. V. *Administrative-Legal Legitimation of Law Enforcement Agencies in the Field of National Security*. Scientific Bulletin of Uzhhorod National University. Law Series – 2025 – Issue 88, Part 2.
15. *Administrative Law of Ukraine. Complete Course: Textbook* / Galunko V., Dikhtiievskyi P., Kuzmenko O., Stetsenko S., Nikitenko O. et al. – 2nd Edition. – Kherson: OLDI-PLUS, 2019. – 520 p.
16. *Law of Ukraine "On the State Border of Ukraine"* // Bulletin of the Verkhovna Rada of Ukraine, 1992, No. 2, Article 5.
17. Becker, G.S. *The Economics of Crime*. Crocc Sections, 1995.
18. Albania. *On the Issue of Fighting Organized Crime in the USA*. Problems of Crime in Criminal Offenses in Catholic Countries. Information Bulletin – 1987 – No. 6.
19. Ya. Tatsiy. *Report of the Commission on Law Enforcement Activities at the Plenary Session of the Constitutional Assembly*. Kyiv; 2012.
20. *Code of Ethics for INTERPOL Officials*. URL: https://www.interpol.int/content/download/file PDF
21. Schelling, T. C. *Economic Analysis and Organized Crime*. U.S. President's Commission on Law Enforcement and Administration of Justice. Task Force Report: Organized Crime. Annotations and Consultant Papers. Washington.
22. Galunko V., Dikhtiievskyi P., Berlach A., Nikitenko O. et al. *Administrative Law and Administrative Process. Complete Course: Textbook*, 5th edition / Edited by V. Felyk, V. Galunko. Kyiv, 2025. – 992 p.

23. *Concept of Administrative Law Reform in Ukraine* // Bulletin of the Verkhovna Rada of Ukraine – 1998 – No. 48 – pp. 4–5.
24. Shemshuchenko, Yu. S. *Constitutional Guarantees for Human Protection in Law Enforcement Activities: Conference Materials (Sept 24–25, 1999)*. Kyiv, 1999.
25. *Law of Ukraine "On the State Border Guard Service of Ukraine"* // Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 27, Article 208.
26. Malanchii, M.O. *Formation of Professional Identity among Officers of the Ukrainian Border Guard Service*. Aspects of Public Administration – 2014 – Nos. 3–4.
27. Becker, G.S. *Crime and Punishment* / Edited by G.S. Becker, W.L. Landes. New York, 1974.
28. Nikitenko, O.I. *Theoretical Issues in Enhancing State Internal Security by Law Enforcement Agencies: Monograph*. – Kherson: Kherson State University, 2011. – 448 p.
29. *Legal Doctrine of Ukraine: In 5 Volumes* – Kharkiv: Pravo, 2013. Volume 1: General Theoretical and Historical Jurisprudence / V. Ya. Tatsiy, O. D. Sviatotskyi, S. I. Maksymov et al.; Edited by O. V. Petryshyn – 692 p.
30. *Administrative Law of Ukraine. Complete Course: Textbook* / Edited by V. Galunko, O. Pravotorova. 3rd edition. Kyiv: Academy of Administrative-Legal Sciences, 2020. – 466 p.
31. Verkhovna Rada of Ukraine. (2003). *Law of Ukraine "On the State Border Guard Service of Ukraine" (No. 661-IV)*. URL: https://zakon.rada.gov.ua/laws/show/661-IV (Accessed: July 23, 2025)
32. Kostenko, O. V. (2022). Analysis of national strategies for the development of artificial intelligence. Information and Law, vol. 2(41), pp. 58-69. DOI: https://doi.org/10.37750/2616-6798.2022.2(41).270365