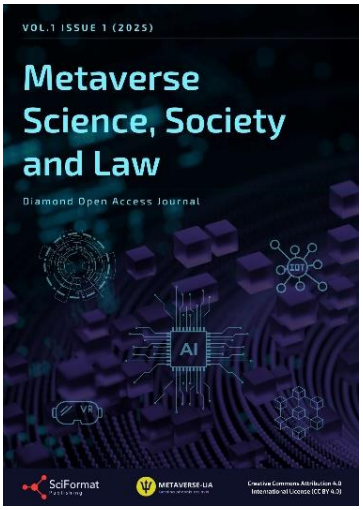

Metaverse Science, Society and Law

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 IN THE FIELD OF INTERNAL INFORMATION SECURITY AS A COMPONENT OF UKRAINE'S NATIONAL SECURITY
ARTICLE INFO	Oleksandr Nikitenko, Illia Zhuravel, Bohdan Krymchanin, Andrii Verbitskyi. (2025) Legal Regulation in The Field of Internal Information Security as a Component of Ukraine's National Security. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.15
DOI	https://doi.org/10.69635/mssl.2025.1.1.15
RECEIVED	30 April 2025
ACCEPTED	10 July 2025
PUBLISHED	16 July 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

LEGAL REGULATION IN THE FIELD OF INTERNAL INFORMATION SECURITY AS A COMPONENT OF UKRAINE'S NATIONAL SECURITY

Oleksandr Nikitenko
Doctor of Juridical Sciences, Professor, Honored Lawyer of Ukraine, Ukraine
ORCID ID: 0009-0001-6572-4072

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

Bohdan Krymchanin
Third-Year Higher Education Student, The State Tax University, Ukraine
ORCID ID: 0009-0003-4339-6658

Andrii Verbitskyi
Third-Year Higher Education Student, The State Tax University, Ukraine
ORCID ID: 0009-0006-6031-3473

ABSTRACT

Legal regulation in the field of national information policy is guaranteed by the Constitution of Ukraine [1], the Resolution of the Verkhovna Rada of Ukraine "On the Concept (Fundamentals of State Policy) of National Security of Ukraine," the Law of Ukraine "On Information," the Law of Ukraine "On the Protection of Information in Information and Telecommunication Systems," the Presidential Decree enacting the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy," and other regulatory and subordinate legal acts [2].

Scientific research on ensuring state security in Ukraine's border regions is wide-ranging, particularly in safeguarding information security against unlawful intrusions. The protection of sovereignty and territorial integrity, as well as the provision of economic and information security, are among the most crucial responsibilities of the state and the shared duty of the Ukrainian people. It should be noted that the responsibility for maintaining national security and securing the state border in the domain of information security lies with the relevant government authorities, military formations, and law enforcement agencies, whose structure and operational procedures are defined by law [3].

Furthermore, reform initiatives in Ukraine's law enforcement sector and the formalization of law enforcement agencies in the Constitution require, first and foremost, clarification of the term "law enforcement agencies," an understanding of their functional purpose, and based on that, the definition of their system. At present, Ukrainian administrative law recognizes anywhere from 17 to 80 law enforcement agencies, depending on the particular interpretation of the "law enforcement function" and the classification criteria built upon it [4].

Current legislation does not provide a comprehensive concept of law enforcement agencies. Instead, it defines them by way of enumeration. Additionally, the Law of Ukraine "On State Protection of Court Employees and Law Enforcement Officials" dated December 23, 1993 expands this list to include other executive bodies—such as the Fisheries Protection Service and the State Forest Protection Service—which perform not only law enforcement functions but also contribute to legal regulation in the field of internal information security.

KEYWORDS

Information Security, Rule of Law, Legal Provision, National Security, Artificial Intelligence, Sovereignty, Metaverse

CITATION

Oleksandr Nikitenko, Illia Zhuravel, Bohdan Krymchanin, Andrii Verbitskyi. (2025) Legal Regulation in The Field of Internal Information Security as a Component of Ukraine's National Security. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.15

Introduction.

In today's information society, the development of national information policy has become a priority area of state governance, particularly in the context of ensuring internal security. A decisive factor shaping this process is the current special Ukrainian legislation, which integrates provisions of international law, European law, and national priorities. In this context, the issue of a comprehensive analysis of the legal and regulatory foundations governing the information sphere — especially in terms of national security and human rights — becomes increasingly relevant.

The prerequisites for this research stem from the need to reassess approaches to the legal regulation of the information space, taking into account the challenges posed by hybrid warfare, cyber threats, the spread of disinformation, and technological transformations, particularly the rapid development of artificial intelligence. The use of intelligent systems that automate personal data processing, carry out information monitoring, or participate in decision-making raises new ethical and legal issues requiring systematic academic analysis.

In addition, the rapid evolution of digital technologies—including the Internet of Things, big data, cloud computing, and especially artificial intelligence—creates novel legal challenges. Contemporary intelligent systems are capable not only of processing vast volumes of personal data automatically, but also of analyzing user behavior, forecasting social trends, influencing electoral sentiments, shaping public opinion, and even participating in strategic decision-making in both administrative governance and defense sectors.

In this context, a range of ethical and legal issues emerges, such as the protection of privacy, ensuring algorithmic transparency, guaranteeing human rights, preventing discrimination, and assigning accountability for decisions made by artificial intelligence systems [5].

Since the mid-20th century, the rapid development of information technologies has taken on a global scale. By the early 2000s, the global information industry had reached USD 3 trillion. This affirms the rapid emergence of the information society worldwide. Its defining feature is that information has become a strategic resource capable of interacting not only with the material world but also with the spiritual realm of individuals. That is why the section "Information Society" was included as a fundamental part of Ukraine's European Union integration program [6].

The formation of the information society is currently strengthened by the shift from two-dimensional cyberspace to multi-dimensional immersive ecosystems — Metaverse, where data, identities, and legal relations exist in the form of digital avatars, tokenized assets, and virtual territories. Consequently, there is a growing need for a concept of "Digital Sovereignty 2.0," which encompasses not only classical aspects of control over national information traffic but also management of cross-border XR-content streams, transactions within smart contracts, and seamless verification of citizens' "digital identity" in virtual reality environments.

A new vision is emerging regarding Ukraine's primary source of national strength — namely, that in the 21st century, the key factor is information and the state's ability to possess and employ advanced information technologies and tools to efficiently process, store, transmit, and disseminate necessary information. Such capacity enables the protection of Ukraine's sovereignty and territorial integrity, as well as the guarantee of its economic and informational security — key functions of the state and a shared responsibility of the Ukrainian people.

Ensuring national security and protecting Ukraine's state border is entrusted to the appropriate military units and law enforcement agencies, whose organization and procedures are defined by law. According to Part 1, Article 2 of the Law of Ukraine "On Information," the core principles include: 1) guarantee of the right to information; 2) openness, accessibility of information, freedom of information exchange; 3) reliability and completeness of information; 4) freedom of expression and belief; 5) legality of obtaining, using, disseminating, storing, and protecting information; 6) protection of individuals from interference in their personal and family life [7].

The primary objective of this study is to define the role of information legislation in ensuring national security and in shaping a balanced policy that guarantees respect for human rights, including the freedoms of speech, assembly, and access to information — while taking into account the challenges posed by the digital age and artificial intelligence. The scope of the research encompasses legal aspects of the functioning of mass media, telecommunications, electronic commerce, personal data processing, and intellectual property. The anticipated contribution lies in proposing strategic directions for improving national information policy in accordance with international standards and technological advancement.

Part 1: Artificial Intelligence in Ukraine: Development Potential, Challenges, and Its Impact on Regulation in the Field of Information and Internal State Security

In the 21st century, artificial intelligence (AI) is emerging as a key technology that fundamentally transforms the operational principles of law enforcement agencies, the Armed Forces of Ukraine, and government institutions tasked with protecting sovereignty and territorial integrity, ensuring economic and information security, safeguarding state security, securing the national border, and maintaining public order in Ukraine—as all citizens possess equal constitutional rights and freedoms and are equal before the law. It is important to note that the integration of artificial intelligence is only gaining momentum, yet it already demonstrates significant potential and relevance. Notably, digital transformation is gradually encompassing strategically vital sectors such as the economy, information infrastructure, law enforcement systems, sovereignty protection, territorial integrity, national security, and border defense.

At the current stage, artificial intelligence in Ukraine is transitioning from theoretical research to practical application in the legal regulation of internal information security. An increasing number of Ukrainian enterprises and governmental institutions are adopting machine learning algorithms, natural language processing, image recognition, and predictive analytics. For instance, the banking sector already employs systems for automated risk assessment, fraud detection, and personalized customer service. In the healthcare field, AI-based solutions are used for analyzing medical images, early disease diagnostics, and optimizing physician workload.

Artificial intelligence (AI) plays a particularly important role in the sphere of national information security and in the legal regulation of Ukraine's security framework. The automation of administrative processes aimed at ensuring state security, as part of legal system reform, seeks to fully realize constitutional principles, the organization of state governance, the rule of law and legality, and the humanistic standards of government activity. Addressing these tasks requires engagement across various branches of law, but decisive contributions must come from such fundamental domains of public law as constitutional law, information law, and administrative law [8]. Within the framework of internal information security, intelligent data analysis, e-governance, and digital citizen identification represent critical steps toward a more effective, transparent, and accessible government. Ukraine's experience launching the digital platform "Diia" has already attracted international attention as an example of successful digital transformation.

In this context, promising initiatives include the deployment of immersive XR-based simulation systems for national security and defense forces: virtual replicas of critical infrastructure or urban agglomerations enable multi-stage threat simulations and real-time response scenarios to disinformation campaigns, cyberattacks, and terrorist incidents. Legally, these developments give rise to a series of new challenges — specifically, concerning the procedural status of data generated in such "digital training grounds" and its admissibility as evidence in criminal and administrative proceedings.

One of the key issues hindering the development of artificial intelligence in Ukraine is the outflow of intellectual capital. Many talented IT professionals, machine learning engineers, and researchers leave the country in pursuit of better career opportunities, higher salaries, and more stable research environments. Another significant obstacle is the absence of a coherent national strategy for AI development and implementation. At the national level, no unified concept or regulatory document has yet been adopted to establish priorities, regulatory principles, or support mechanisms for the sector. This vacuum results in legal uncertainty, complicating business planning and discouraging scientific initiatives.

The growth of AI is also seriously limited by inadequate access to high-quality open data. Effective functioning of modern algorithms requires large volumes of structured, accurate, and current data. Yet both the public and private sectors continue to show low levels of data transparency and standardization, which prevents the full training and testing of intelligent systems.

It is worth noting that certain aspects of legal regulation related to state security have been the subject of dissertation research by scholars such as V. B. Averyanov, O. M. Bandurka, O. L. Kopelenko, O. I. Nikitenko, O. F. Opryzhko, I. V. Aristova, R. A. Kolyuzhny, V. Ya. Tatsiy, N. E. Nyzhnyk, O. V. Kostenko and others. Recently, increased attention has been paid to problems in the legal regulation of internal information security. Among notable domestic scholars are Yu. P. Bytyak, V. M. Bevzenko, V. V. Halunko, S. V. Kivalov, T. O. Kolomoiets, V. K. Kalpakov, A. M. Kulish, R. S. Melnyk, O. M. Muzychuk, Yu. S. Shemshushenko, and other researchers.

In the science of administrative law and in the sphere of legal regulation of internal information security, conceptual and methodological foundations of the administrative-legal nature of state security remain insufficiently explored — especially regarding legal regulation and state control in the information and

communication domain. This set of issues determines the relevance of this study and creates the conditions for the development of a new administrative-legal paradigm for safeguarding national security and regulating the sphere of national information security, taking into account both domestic and international experience.

Part 2: Legal Regulation and the Use of Artificial Intelligence in Law Enforcement Activities for Ensuring Information Security

A legal state and civil society must guarantee individuals maximum freedom and the free development of their personality. Achieving this requires that the legal order within the state and society is upheld on certain principles enshrined in the Constitution and laws of the country—specifically principles of democracy, humanism, social justice, constitutionalism, the rule of law, and legality. In today's environment of ever-increasing digital information, technologies, and threat complexity, state and law enforcement agencies are confronted with the need to process massive volumes of data, detect hidden patterns, and respond effectively to internal and external threats. In this context, the integration of artificial intelligence into the activities of the National Police of Ukraine [9], the Security Service of Ukraine [10], the State Border Guard Service of Ukraine [11], and other law enforcement agencies becomes a crucial factor in transforming the national security system.

One of the key areas is the analysis of big data using machine learning algorithms. These technologies enable automated detection of suspicious transactions, financial abuse, money laundering schemes, and the tracing of connections among participants in criminal activities. For example, systems can identify discrepancies between declared incomes and actual expenditures of public officials, which can serve as grounds for initiating corruption proceedings.

Another promising area is the use of facial recognition systems based on computer vision. Surveillance cameras integrated with such algorithms are capable of detecting and identifying suspected individuals in real time in crowds, at train stations, airports, or near government facilities. This significantly enhances the effectiveness of counter-terrorism efforts, the search for wanted persons, and the prevention of public threats.

AI also enables the development of crime prediction models. These systems analyze historical data — location, time, circumstances of offenses—and generate forecasts of high-risk zones. This approach allows law enforcement to plan patrol routes more effectively, optimize the allocation of forces and resources, and prevent offenses before they occur.

Furthermore, artificial intelligence technologies are actively used in digital forensics. Software can automatically process large volumes of electronic evidence — including emails, messaging apps, files, and media — by filtering, classifying, and retrieving relevant information. This significantly accelerates investigations and allows human resources to focus on strategically important tasks.

Alongside the advantages of using AI in the security sector, new risks also emerge. These include potential algorithmic bias if systems are trained on flawed or unbalanced data; false positives in facial recognition technologies; and a lack of transparency in decision-making, which may infringe on citizens' rights and freedoms. Particularly pressing is the issue of the legal use of such technologies — especially in matters of privacy, personal data processing, and the right to protection.

In light of this, it is extremely important to establish clear ethical standards, regulatory acts, and mechanisms for public oversight of AI use in the field of law enforcement. It is essential that every technology implemented in this domain undergo expert review, is tested for compliance with international human rights standards, and is integrated strictly within the framework of existing legislation.

Thus, artificial intelligence opens new horizons in the operations of Ukrainian law enforcement agencies by enhancing their responsiveness, precision, and efficiency. At the same time, its implementation requires a careful, responsible, and balanced approach in order to safeguard both security and the protection of citizens' rights and freedoms.

Part 3: State Information Security Amid Hybrid Warfare

Information security has become one of the key components of Ukraine's national security in the context of hybrid warfare, which includes not only armed conflict but also massive information-psychological, cyber, and media pressure. Since the onset of armed aggression by the Russian Federation, Ukraine's information space has become a primary battlefield, where strategic importance lies not only in data flow control but also in the ability to detect, analyze, and neutralize information threats.

In today's digital environment, artificial intelligence tools have become critically important for ensuring effective protection of the information space. Information security is no longer limited to technical safeguarding of communication channels or computer systems. It now encompasses a wide range of tasks,

including monitoring the information environment, combating disinformation, detecting cyberattacks, managing reputational risks, and securing digital sovereignty.

Cyberattacks on critical infrastructure — such as energy enterprises, banks, transportation hubs, telecommunications nodes, healthcare facilities, and state registries — take center stage. Malicious actors use advanced tactics, ranging from phishing to deploying complex malware capable of compromising data integrity or fully paralyzing the functioning of the country's information and communication systems.

Equally dangerous is disinformation and the spread of fake news aimed at inciting panic, eroding trust in authorities, undermining public morale, or sowing discord among various social groups. Modern technologies allow the creation of highly convincing fake messages and videos (including deepfakes), which are distributed automatically via bot networks on social media. There is also evidence of interference in electoral processes and manipulation of public opinion. Through big data analytics, microtargeting, and manipulative content, it becomes possible to influence electoral behavior, shape biases, and fuel radical sentiments.

Another facet is cyber espionage and the leakage of confidential information. This refers to unlawful intrusion into state information systems to steal strategic intelligence, defense plans, diplomatic correspondence, or critical communications. Ukraine is actively investing in next-generation cybersecurity systems based on machine learning algorithms. These systems not only detect suspicious activity in real time but also respond adaptively to new types of attacks, blocking intrusions before they cause serious damage. Neural networks help identify atypical traffic patterns or attempts to bypass protection that may go unnoticed by traditional monitoring systems.

A particularly significant threat amid hybrid warfare is posed by manipulative narratives disseminated through social VR platforms, where users interact in immersive presence modes. Adversaries are capable of creating "cyber-enclaves" — closed virtual spaces where psychological influence, recruitment, or hacktivism coordination takes place. Detection and neutralization of such cells require synergy between cyber intelligence, cognitive linguistics, and behavioral digital footprint analysis—tasks executed by hybrid AI systems trained on multichannel data (VR telemetry, biometrics, voice patterns). The legal codification of "immersive counter-surveillance" procedures would introduce legitimate mechanisms for authorized bodies to access closed VR environments, ensure proportionality in privacy interventions, and apply sanctions against administrators of international platforms who ignore lawful requests [12].

Network monitoring and automated content filtering allow for rapid identification of disinformation sources, analysis of their origin and impact, and implementation of blocking measures. This is especially effective in coordinating information campaigns where bots or trolls disseminate synchronized narratives.

AI-powered fact-checker bots play a distinct role. They scan media, social networks, and messaging platforms, comparing shared statements with verified sources, databases, and official information. Thanks to these technologies, it is possible to swiftly counter fake news and reduce its influence on public consciousness.

A crucial step in structuring Ukraine's information security system was the establishment of the National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine. This body oversees coordination among governmental, military, diplomatic, and civilian entities on cybersecurity matters and collaborates with international partners and the private sector.

The Center participates in the development of cyber training grounds, conducts expert simulations of response scenarios to complex attacks, and promotes information hygiene programs among the population aimed at raising awareness of manipulative technologies and encouraging safe digital behavior.

Conclusions.

In an era of rapid digitalization, where data transforms into a new form of resource and algorithms become drivers of decision-making, the role of artificial intelligence in the national security system and information protection is growing exponentially. Ukraine, as a state undergoing both technological modernization and civilizational confrontation, bears a unique historical mission — to develop a model for the use of artificial intelligence that is simultaneously effective, lawful, and humanistic. Today, AI is increasingly employed in combating cybercrime, terrorism, financial fraud, corruption, and information aggression. It assists not only in detecting threats but also in predicting their emergence and acting proactively. At the same time, intelligent technologies are becoming instruments of attack, manipulation, and interference — necessitating development not only in cybersecurity, but also in digital ethics, legal regulatory mechanisms, and a high level of legal culture within society. A democratic and open state must not allow the uncontrolled use of AI to violate citizens' constitutional rights or create digital inequality. Thus, the future of effective and secure state functioning in the context of hybrid threats directly depends on how responsibly,

deliberately, and thoughtfully Ukraine develops its digital technologies. The creation of a national model of ethical artificial intelligence, reinforced by public oversight and international partnership, can become not only a tool of internal protection, but also a model for other nations in shaping a secure digital world. In summary, Ukrainian governmental and law enforcement bodies play a leading role in the legal regulation and provision of internal information security against internal and external threats, the spread of corruption, bribery, collusion between business and politics, organized crime, international terrorism, manifestations of separatism, the emergence of ethnic and interreligious conflict, and the unlawful use of information—all of which contribute to national security, especially during the years of Russia's full-scale invasion of Ukraine (February 24, 2022). The law enforcement system, as an object of study, is a complex state-legal phenomenon explored by various disciplines that perform law enforcement functions in regulating internal information security—undertaken by governmental authorities, law enforcement agencies, and the Armed Forces of Ukraine—within the framework of improving legal regulation under administrative law, not only at the state level but also by local self-government bodies.

REFERENCES

1. Constitution of Ukraine of June 28, 1996 No. 254k/96-VR // Official Bulletin of the Verkhovna Rada of Ukraine – 1996 – No. 30 – Article 141.
2. Nikitenko O. I. Theoretical Problems of Improving State Internal Security by Law Enforcement Agencies: Monograph. – Kherson: Kherson State University, 2011 – p. 400.
3. Averyanov V. B. Commentary on the Constitution of Ukraine / V. B. Averyanov [et al.]; edited by V. F. Opryshko [et al.]; Verkhovna Rada of Ukraine, Institute of Legislation. – Kyiv: [n.p.], 1996. – 368 p.
4. Report of the Commission on Law Enforcement Activities at the Plenary Session of the Constitutional Assembly. – Kyiv, 2012.
5. Legal Doctrine of Ukraine: in 5 vols. – Kharkiv: Pravo, 2013. Vol. 1: General Theory and Historical Jurisprudence / V. Ya. Tatsiy, O. D. Svyatotskyi, S. I. Maksymov et al.; edited by O. V. Petryshyn – p. 692.
6. Program of Ukraine's Integration into the European Union // Official Bulletin of the Verkhovna Rada of Ukraine – July 10, 2015.
7. Law of Ukraine "On Information": as of December 1, 2002. Official publication. Kyiv: Parliamentary Publishing House, 2002 – 24 p.
8. Concept of the Reform of Administrative Law of Ukraine // Official Bulletin of the Verkhovna Rada of Ukraine – 1998 – No. 48 – pp. 4–5.
9. On the National Police: Law of Ukraine of July 2, 2015 No. 580-VIII; as of August 16, 2024. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (accessed: July 4, 2025).
10. Law of Ukraine "On the Security Service of Ukraine" // Official Bulletin of the Verkhovna Rada of Ukraine (OBVR), 1992, No. 27, Article 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text
11. Law of Ukraine "On the State Border Guard Service of Ukraine" // Official Bulletin of the Verkhovna Rada of Ukraine (OBVR), 2003, No. 27, Article 208. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text
12. Oleksii Kostenko, Dmytro Zhuravlov, Volodymyr Nikitin, Volodymyr Manhora, Tamila Manhora, Ivan Gabani. A Typical Cross-Border Metaverse Model as a Counteraction to Its Fragmentation. (2024). Bratislava Law Review, 8(2), pp. 163–176. https://doi.org/10.46282/blr.2024.8.2.844