RICA – v. 9, n. 14, 2025
Revista Interdisciplinar de Ciência Aplicada
ISSN: 2525-3824

Forecasts of transformation in legal regulation of artificial intelligence for cybersecurity in Ukraine's defence sector

Oleh Semenenko (oleh-sem@ukr.net)
Central Research Institute of the Armed Forces of Ukraine

Nataliia Shynkaruk (natali.shyn@outlook.com)
National University of Life and Environmental Sciences of Ukraine

Polina Tolok (polina.tolok@hotmail.com)
National Defence University of Ukraine

Serhii Ostrovskyi (serostrovskyi@outlook.com)
Central Research Institute of the Armed Forces of Ukraine

Ihor Davydov (Ihor_Davydov@hotmail.com)
Central Research Institute of the Armed Forces of Ukraine

DOI: 10.18226/25253824.v9.n14.02

Submitted on: 02/06/2024 **Revised on:** 23/12/2024 **Accepted on:** 01/08/2025

Abstract: The integration of artificial intelligence (AI) systems into cybersecurity strategies in Ukraine's defence sector presents significant opportunities and challenges, particularly in the context of legal regulation. This article addresses the urgent need to establish a comprehensive framework for the legal regulation of AI in cybersecurity. It systematizes the factors influencing the adaptation of legal norms to the rapid development of AI technologies and evaluates their potential implications. A combination of general scientific and specialized legal methods was used, including a comparative analysis of international practices, a systemic and structural examination of the interaction between legal frameworks and AI capabilities, as well as legal modelling and forecasting techniques. An expert survey of 30 specialists in cybersecurity, law, and national security revealed critical gaps in Ukrainian legislation. These include the absence of a legal definition and classification of AI systems, undefined liability for autonomous system decisions, and the lack of certification standards for AI technologies in cybersecurity. The study developed a Legal Risk Assessment Matrix, identifying the most critical risks, such as the violation of human rights, including freedom of expression. Recommendations for updating Ukrainian legislation were proposed, including amendments to existing laws and the formulation of a draft law titled "On the Regulation of Artificial Intelligence in National Security and Defence." Mechanisms for ensuring algorithmic transparency and protecting critical infrastructure were outlined, emphasizing ethical AI use and protocols for human interaction with autonomous systems. The article also explores avenues for international cooperation, particularly in the context of partnerships with NATO and the European Union. The results are intended to inform policymakers and contribute to the formulation of legal and cybersecurity strategies to counter hybrid threats and information warfare.

Keywords: Artificial intelligence; Legal regulation; Cybersecurity; Defence sector; Algorithmic transparency; Hybrid threats; Ethical standards

***Resumo**:* A integração de sistemas de inteligência artificial (IA) nas estratégias de cibersegurança no setor da defesa da Ucrânia apresenta oportunidades e desafios significativos, especialmente no contexto da regulamentação jurídica. Este artigo aborda a necessidade urgente de estabelecer um quadro abrangente para a regulamentação legal da IA na cibersegurança. Sistematiza os fatores que influenciam a adaptação das normas jurídicas ao rápido desenvolvimento das tecnologias de IA e avalia as suas potenciais implicações. Foi utilizada uma combinação de métodos científicos gerais e jurídicos especializados, incluindo uma análise comparativa das práticas internacionais, um exame sistêmico e estrutural da interação entre os quadros jurídicos e as capacidades de IA, bem como a modelização jurídica e as técnicas de previsão. Um inquérito realizado a 30 especialistas em cibersegurança, direito e segurança nacional revelou lacunas críticas na legislação ucraniana. Estas incluem a ausência de uma definição e classificação jurídica dos sistemas de IA, a responsabilidade indefinida para decisões de sistemas autônomos e a falta de normas de certificação para tecnologias de IA em segurança cibernética. O estudo desenvolveu uma Matriz de Avaliação de Riscos Legais, identificando os riscos mais críticos, como a violação dos direitos humanos, incluindo a liberdade de expressão. Foram propostas recomendações para a atualização da legislação ucraniana, incluindo alterações às leis existentes e a formulação de um projeto de lei intitulado "sobre a regulamentação da inteligência artificial na segurança e defesa nacional". Foram delineados mecanismos para garantir a transparência algorítmica e proteger as infraestruturas críticas, enfatizando a utilização ética da IA e dos protocolos para a interação humana com sistemas autônomos. O artigo explora também caminhos para a cooperação internacional, particularmente no contexto das parcerias com a NATO e a União Europeia. Os resultados pretendem informar os decisores políticos e contribuir para a formulação de estratégias jurídicas e de cibersegurança para combater as ameaças híbridas e a guerra de informação.

Palavras-Chave: Inteligência artificial; Regulamentação legal; Cibersegurança; Setor de defesa; Transparência algorítmica; Ameaças híbridas; Padrões éticos.

Introduction

In the current environment of rapid technological development and geopolitical changes, legal regulation of the use of artificial intelligence (AI) in the defence sector is becoming key to national security. This problem is particularly acute for Ukraine, which is at the forefront of defending democratic values and territorial integrity in the face of hybrid warfare and constant cyberthreats [1-3]. The rapid development of AI technologies opens unprecedented opportunities for strengthening cyber defence, but at the same time poses complex challenges for the legal system, which must strike an adequate balance between innovation and ethical compliance, between strengthening national security and protecting fundamental human rights. The relevance of the study of legal aspects of AI use for ensuring cybersecurity of the Ukrainian defence sector is conditioned by the urgent need to develop an effective, flexible, and comprehensive legal framework. Such a framework should not only meet modern technological realities and international standards, but also consider the unique context of Ukraine as a state that actively counteracts hybrid threats [4].

The multifaceted nature of AI in defence cybersecurity has attracted considerable attention from researchers around the world. A comprehensive review of the recent literature reveals a diverse range of perspectives and conclusions on this issue. Taddeo et al. [5] and Kaushik et al. [6] have explored the ethical implications of AI-driven cybersecurity systems, highlighting the need for robust governance frameworks to ensure responsible deployment in defence contexts. Their study highlighted the potential risks of autonomous decision-making in critical infrastructure, calling for strict oversight mechanisms. Building on this framework, Usman et al. [7] conducted an in-depth study of the legal challenges associated with AI in cybersecurity, particularly relevant to emerging economies and regions facing geopolitical tensions. Their findings highlighted the significance of developing a comprehensive legal framework that addresses the unique challenges posed by the use of AI in cybersecurity. Kanellopoulos [8] and Kant [9] studied the implications of AI and machine learning in cyber intelligence, focusing on the legal aspects of data sharing and cross-border cooperation. Their study highlighted the need to harmonise international legal standards to promote effective cybersecurity cooperation while protecting national sovereignty.

Margulies [10] thoroughly explored the complex interrelationships between AI, cybersecurity, and international law, raising critical questions about the applicability of existing legal norms to AI-driven cyberoperations in conflict situations. His study prompted a reassessment of conventional legal concepts in the context of innovative technologies, identifying gaps in existing international law that need to be addressed. Adding to this perspective, Haner and Garcia [11] explored the legal and ethical implications of autonomous cyber capabilities, pointing to the challenges of attribution and accountability in AI-enabled cyber operations. Their study highlighted the need for clear legal guidelines governing the use of AI in offensive and defensive cybersecurity measures. Considering the concrete context of critical infrastructure protection, Radanliev et al. [12] provided a comprehensive review of AI and robotics in cyber risk insurance, with implications for the national security and defence sectors. Their study identified considerable challenges in assessing and mitigating the risks associated with AI-based cybersecurity systems, highlighting the need for adaptive legal and regulatory frameworks.

Singh et al. [13] thoroughly reviewed the transformative potential of AI in enhancing cyber resilience, who proposed a framework for integrating AI into the security of industrial control systems. Although their study did not specifically focus on the defence sector, it provided valuable insights into the regulatory challenges of implementing AI-based security measures in sensitive infrastructure. Expanding on this theme, Smuha [14] explored the European Union's (EU) approach to AI regulation, including its application in cybersecurity and defence. Her analysis offered valuable perspectives on balancing innovation with ethical and legal considerations that could inform Ukraine's approach to AI governance in the defence sector. In a groundbreaking study, Dwivedi et al. [15] and Gillespie et al. [16] conducted a multi-country investigation of AI adoption and effectiveness in the public sector, including applications in defence and cybersecurity. Their research highlighted the varying degrees of legal readiness in different countries, emphasising the need for Ukraine to develop a robust and adaptive legal framework.

Despite these considerable contributions, several critical gaps persist in the current body of knowledge. The concrete legal challenges that Ukraine faces in implementing AI for defence cybersecurity have not yet been comprehensively addressed. Furthermore, the rapid pace of technological progress requires a constant reassessment of the legal framework to ensure its relevance and effectiveness. However, despite the considerable amount of research conducted, there is still a series of understudied aspects that require further analysis and development. Specifically, the issue of adapting Ukrainian legislation to the challenges associated with the use of AI in the context of hybrid warfare and the constant cyber threat requires a more in-depth investigation. There is an urgent need to develop a comprehensive approach that accommodates both the technical capabilities of AI to enhance cyber defence and the potential risks of its misuse. The mechanisms of international cooperation in the field of legal regulation of AI for cybersecurity are understudied, especially in the context of Ukraine's Euro-Atlantic integration and the need to harmonise national legislation with EU and North Atlantic Treaty Organisation (NATO) standards. Furthermore, there is a need to develop a methodology for assessing the effectiveness of legal norms in a rapidly changing technological environment, which will allow prompt adaptation of legislation to new challenges and opportunities of AI.

The purpose of this study was to develop a conceptual model of legal regulation of the use of AI in the cybersecurity system of the defence sector of Ukraine, which would consider modern technological capabilities, international legal norms, and the specifics of the country's national security. The objectives of this study were as follows:

1. To conduct a comparative analysis of international experience in legal regulation of AI in cybersecurity, with a particular focus on the practices of countries facing national security challenges analogous to Ukraine.

2. To research the relationship between AI technological capabilities in cybersecurity and existing legal norms in

Ukraine, identifying potential gaps and contradictions in the current legislation.

3. To develop a methodology for assessing legal risks associated with the introduction of AI systems in the cybersecurity of the defence sector, considering the specifics of hybrid threats and information warfare.

4. To formulate a proposal for adapting Ukraine's national legislation to effectively regulate the use of AI in cybersecurity, including mechanisms to ensure transparency of algorithms and protection of critical infrastructure.

Materials and Methods

The research methodology included general scientific and specialised legal methods, which ensured a comprehensive and objective analysis. The dialectical method was used to investigate the legal regulation of the use of AI in cybersecurity as a dynamic phenomenon that changes under the influence of technological and geopolitical factors. The systemic-structural method helped to explore the relationship between the elements of legal regulation and the technological capabilities of AI. The comparative legal method was used to analyse international practices based on regulations, scientific publications, and official reports of international organisations for 2019-2024, with a focus on the practices of NATO and countries with national security challenges analogous to Ukraine. Specifically, the National Artificial Intelligence Initiative Act [17] and the Regulation (EU) No. 2024/1689 of the European Parliament and of the Council "Laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828" (Artificial Intelligence Act) [18] were analysed. The formal legal method was used to analyse and interpret legal provisions.

The method of legal modelling was employed to investigate the relationship between the technological capabilities of AI and the existing legal norms of Ukraine. The analysis was based on the Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [19], the Cybersecurity Strategy of Ukraine [20], the Law of Ukraine No. 2469-8 "On National Security of Ukraine" [21], the Law of Ukraine No. 2297-6 "On Personal Data Protection" [22], the Law of Ukraine No. 3855-12 "On State Secrets" [23], as well as other relevant regulations. The method of legal forecasting combined with risk analysis was used to develop a methodology for assessing the legal risks associated with the introduction of AI systems in the cybersecurity of the defence sector.

The study employed the methods of law-making experiment and legal construction to formulate proposals for the adaptation of the national legislation of Ukraine. This helped to develop concrete mechanisms to ensure the transparency of AI algorithms and protect critical infrastructure. A Venn diagram was created to visualise the correlation between the technological capabilities of AI in cybersecurity and the existing legal regulation in Ukraine.

A prominent component of the study was an expert survey conducted to validate the developed proposals and assess potential legal risks. The survey involved 30 experts, including 10 cybersecurity experts, 10 lawyers specialising in AI legal regulation, and 10 national security specialists. The criteria for selecting experts were as follows: at least five years of professional experience in the relevant field, publications on the research topic, participation in the development of regulations or strategic documents in the field of cybersecurity and AI. The survey was conducted on the online platform SurveyMonkey with the use of using a customised questionnaire containing 20 closed-ended questions rated on a five-point Likert scale, where 1 means "strongly disagree" and 5 means "strongly agree". This scale helped to assess the degree of agreement among experts with various statements regarding the legal regulation of AI in cybersecurity, potential risks, and priority areas for improving legislation. In addition, the questionnaire contained five open-ended questions to receive detailed comments and suggestions. Experts received questionnaires via email with a personal invitation to take part.

To assess the identified legal risks, a system of criteria was developed that accommodates the specifics of hybrid threats and information warfare. These criteria include two main assessment parameters: the probability of the risk occurring and the severity of the consequences. This approach allows not only qualitative but also quantitative assessment of each of the identified risks, which is critical for making informed decisions on the implementation of AI systems in the defence sector.

The ethical aspects of the study were ensured by obtaining informed consent from all survey participants. The experts were informed about the objectives of the study, the voluntary nature of participation, and the possibility to withdraw at any stage. All data was anonymised to protect confidentiality.

Results

The rapid development of AI technologies and their integration into cybersecurity systems open new opportunities to protect Ukraine's critical infrastructure and national interests. This is vital for the defence sector, where the effectiveness of cyber defence directly affects national security. At the same time, the introduction of AI in cybersecurity poses a series of legal challenges that require detailed analysis and resolution. The study focused on the legal aspects of using AI for cybersecurity in the defence sector of Ukraine. It included an analysis of international experience in regulating AI, an assessment of the compliance of Ukrainian legislation with modern technologies, and the identification of legal risks associated with the introduction of AI in cyber defence.

In the context of the rapid development of AI technologies and growing cyberthreats, the analysis of international practices in the legal regulation of the use of AI in cybersecurity is of critical significance for Ukraine. Considering the unique challenges faced by Ukraine in national security, investigating and adapting the best international practices is a key element in developing an effective cyber defence strategy. The world's leading countries are actively developing and implementing specialised legislation to regulate AI in the field of cybersecurity. Specifically, the United States of America (USA) adopted the National Artificial Intelligence Initiative Act [17], which establishes a framework for the development and application of AI, including in the field of national security. This act defines AI as "machine systems capable of performing tasks that normally require human intelligence". The document emphasises the importance of a balanced approach to the development of AI, considering both its potential benefits and risks to national security. The EU is promoting the Regulation (EU) No. 2024/1689 of the European Parliament and of the Council [18], which aims to create common rules for AI in the EU, including cybersecurity aspects. This draft law proposes a broader definition of AI, including systems that can create content, predictions, recommendations, or decisions that affect the environment with which they interact. The European approach is distinguished by a clear categorisation of AI systems by risk level, which determines the relevant regulatory requirements.

Different jurisdictions lack a single universal approach to legal definitions of AI. For example, in the UK, the National AI Strategy defines it as "technologies that perform tasks that would normally require human intelligence, especially when machines are trained from data on how to perform those tasks" [24]. This definition is broad enough to cover various forms of AI, from simple algorithms to complex neural networks. Canadian legislation focuses on AI's ability to learn and adapt, reflecting a narrower approach focused on advanced forms of AI. This diversity of approaches to the definition of AI poses certain challenges for the international harmonisation of cybersecurity legislation, but at the same time allows each country to adapt the regulatory framework to its specific needs and legal traditions.

In terms of AI application in cybersecurity, most countries identify the following key areas: real-time detection and response to cyberthreats; prediction of potential attacks based on the analysis of large amounts of data; automation of cybersecurity processes, including patching and updating systems; analysis of user behaviour and network traffic to identify anomalies. The experience of Israel, which faces constant cyber threats and is actively implementing AI for preventive detection of attacks and automated response to incidents, is particularly illustrative. The Israeli approach is based on the concept of active defence, where AI is used not only for defence but also for proactive detection and neutralisation of potential threats. This experience could be particularly valuable for Ukraine, considering the similarity of the security challenges faced by both countries.

A prominent aspect of regulation is the establishment of restrictions on the use of AI in cybersecurity. Most of the surveyed countries introduce restrictions on the use of AI for mass surveillance without proper legal grounds; autonomous decision-making by AI without human supervision in critical national security systems; and the collection and processing of personal data beyond what is necessary to ensure cybersecurity. The example of Germany is illustrative, where there is a strict restriction on the use of AI to identify people in public places without a court order. This reflects the desire to balance the effectiveness of cyber defence with the protection of fundamental rights and freedoms. This approach is relevant in the context of the growing debate on the ethical aspects of using AI in national security and the need for public control over these technologies.

There is a growing trend towards requiring transparency of AI algorithms, especially those used in critical cybersecurity areas. France, for example, requires developers to provide detailed documentation on the principles of operation of AI systems used in the public sector. This requirement is aimed at ensuring accountability and auditability of AI systems, which is critical to maintaining public confidence in the use of these technologies in the national security sphere. Furthermore, such transparency helps to identify potential biases in AI algorithms that could lead to discriminatory practices or ineffective cybersecurity solutions.

In the context of using AI in cybersecurity, special attention is paid to data protection. Most countries implement strict requirements to minimise the collection of personal data, limiting it to only the amount necessary for the effective functioning of cyber defence systems; encrypt data processed by AI systems to prevent unauthorised access; and establish clear procedures for deleting data once the purpose of its processing has been achieved. Estonia, known for its innovative digital solutions, has established a requirement for mandatory encryption of all data processed by AI systems in the field of cybersecurity. This approach demonstrates a commitment to ensuring maximum protection of sensitive information, even in case of a potential system breach. Notably, such strict data protection requirements not only increase the overall level of cybersecurity, but also help to strengthen citizens' trust in government institutions that use AI technologies. A comparison of the legal regulation of AI in cybersecurity in different countries is presented in Table 1.

The Table 1 demonstrates the diversity of approaches to regulating AI in cybersecurity in different countries, which helps to identify both common trends and unique aspects of each jurisdiction. This data can serve as a basis for the development of regulations in Ukraine, considering the best international practices and adapting them to the specific needs of the state in the field of cybersecurity. The following practices are particularly relevant to Ukraine:

- development of specialised legislation on AI in cybersecurity that would consider the specifics of Ukraine's security challenges and establish a clear legal framework for the development, implementation, and use of AI systems in this area;

- implementing clear mechanisms for controlling the use of AI in critical infrastructures, including a certification system for AI solutions for cybersecurity and regular audits of their operation;

- assurance of a balance between the efficiency of AI systems and the protection of citizens' rights and freedoms, specifically through mechanisms of public control and transparency in the use of AI for national security purposes;

- promotion of public-private partnerships in the development and implementation of AI for cybersecurity, which will enable the inclusion of the best practices of the private sector and ensure rapid adaptation to new threats;

- establishment of specialised bodies to assess the ethical aspects of using AI in cybersecurity, which would ensure that the use of these technologies follows ethical norms and social values.

The issue of international cooperation in regulating AI in cybersecurity deserves special attention. The study showed that many countries are actively developing bilateral and multilateral mechanisms for exchanging information and best practices in this area. For example, the AI Safety Initiative (AISI), launched by the Cloud Security Alliance (CSA), aims to ensure the security and compliance of AI systems, including the development of standards and best practices for the safe use of AI. Ukraine's participation in such initiatives could help not only to improve the level of cybersecurity of the state, but also to strengthen its international position as an important player in the field of cybersecurity.

Notably, the legal regulation of AI in cybersecurity is a dynamic area that is constantly evolving in response to latest technological opportunities and threats. It is crucial for Ukraine not only to adapt the best international practices, but also to develop its own innovative approach that accommodates the unique context of Ukraine's security challenges. This requires a comprehensive approach that would include legislative initiatives, development of technological infrastructure, training of qualified personnel, and the development of ethical standards for the use of AI in the national security sphere.

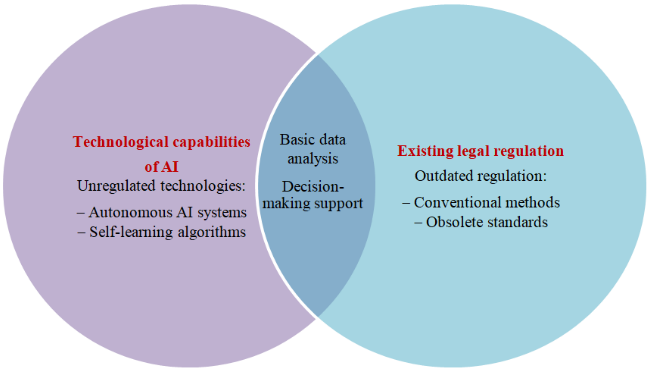
Table 1. Comparative Analysis of Legal Regulation of AI in Cybersecurity in Different Countries

Country	Key regulations	Definition of AI	Principal areas of AI application in cybersecurity	Restrictions on the use of AI	Requirements for algorithm transparency
USA	National Artificial Intelligence Initiative Act (2020)	Systems capable of performing tasks that normally require human intelligence	Threat detection, attack prediction, security automation	Prohibition of use for mass surveillance without a warrant	Mandatory documentation of algorithms for federal systems
United Kingdom	National AI Strategy (2021)	Technologies with the ability to perform tasks that normally require human intelligence	Data analysis, anomaly detection, automated response	Restrictions on autonomous decision-making in critical systems	Regular audits of AI algorithms in the public sector
Germany	AI Strategy (2020)	Systems that demonstrate intelligent behaviour by analysing their environment	Preventive protection, vulnerability analysis, network monitoring	Prohibition on identification of persons in public places without a court order	Mandatory disclosure of training data and algorithmic logic
Estonia	Estonia's national AI strategy (2019, updated 2022)	Computer systems capable of performing tasks that normally require human intelligence	Detection of cyberthreats, analysis of user behaviour, protection of critical infrastructure	Restrictions on the processing of biometric data without consent	Mandatory encryption of all data processed by AI systems in cybersecurity

Source: created by the authors of this study based on National Artificial Intelligence Initiative Act [17], National AI Strategy [25], Artificial Intelligence Strategy of the German Federal Government [26], Estonia's National AI Strategy [27].

There is a significant gap between the rapid development of artificial intelligence technologies in the cybersecurity sector and the current regulatory framework in Ukraine. The study identified several key gaps in AI regulation in the context of cybersecurity in Ukraine. First of all, there is no legislative definition and classification of AI systems, which creates considerable obstacles to effective legal regulation. Specifically, the Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [19] does not contain a definition of AI or its classification in the context of cybersecurity. Article 1 of this Law, which contains definitions of key terms, does not include the concept of AI, which confirms the lack of legal regulation of this technology in the context of cybersecurity. The second key aspect is the legal uncertainty regarding liability for decisions made by autonomous AI systems. An analysis of the current Criminal Code of Ukraine [28] and the Code of Administrative Offences [29] shows that there are no provisions regulating liability for actions committed by autonomous AI systems. For example, Article 361 of the CCU "Unauthorised interference with the operation of electronic computers, automated systems, computer networks, or telecommunication networks" does not consider the specifics of actions taken by AI systems. The third important aspect is the lack of certification and testing standards for AI systems for cybersecurity. A study of the regulatory documents of the State Service for Special Communications and Information Protection of Ukraine (SSSCIP) revealed the absence of special requirements for AI systems used in cybersecurity. This creates risks of using unreliable technologies. It is recommended to amend the aforementioned legislative acts to include a definition of AI and its classification, develop special legislation to regulate AI in the field of cybersecurity, and introduce standards for certification and testing of AI systems for cybersecurity. The Venn diagram presented in Figure 1 clearly shows the areas with a match between technological capabilities and legal regulation and identifies gaps in regulation and technological capabilities that are not currently addressed in the legislation.

Figure 1. Correlation of AI Technological Capabilities and Legal Regulation in Ukraine



Source: created by the authors of this study based on Baranov et al. [30].

A significant mismatch between the technological capabilities of AI and the existing legal regulation in Ukraine was identified. Specifically, the use of autonomous AI systems and self-learning algorithms in cybersecurity stays outside the legal framework. From a legal standpoint, this creates potential risks for national security and may lead to inefficient use of advanced technologies in the defence sector. On the other hand, some of the existing legal regulation relates to outdated methods and standards that do not consider the modern capabilities of AI. This demonstrates the need for a comprehensive update of the regulatory framework in the field of cybersecurity, taking the modern technological reality into account.

It also revealed the unresolved issues of personal data protection when using AI to analyse cyberthreats. The Law of Ukraine No. 2297-6 “On Personal Data Protection” [22] does not contain any special provisions on the processing of personal data by AI systems in the context of cybersecurity. From a legal perspective, this requires amending the legislation on personal data protection to establish special rules and guarantees for data processing by AI systems for cybersecurity purposes.

There is an urgent need to adapt Ukrainian legislation to the challenges posed by the use of AI in cybersecurity. It is necessary to develop a comprehensive legal framework that would define the legal status of AI systems in the context of cybersecurity, establish clear boundaries of responsibility for the actions of autonomous systems, regulate the processes of data collection and processing by AI systems, considering the requirements for personal data protection, and create mechanisms for certification and quality control of AI systems for cybersecurity. Another prominent aspect is the integration of ethical principles of AI in cybersecurity into the legal system. From a legal standpoint, this can be achieved by adopting a special law on the use of AI in cybersecurity or by amending existing regulations accordingly.

An analysis of international experience shows that many countries have already begun the process of adapting their legislation to the challenges of AI in cybersecurity. Specifically, the EU’s experience in developing a comprehensive approach to AI regulation, including cybersecurity aspects, can serve as a guide for Ukraine in developing its own regulatory framework. This should accommodate the specifics of the Ukrainian situation, including the needs of the defence sector and existing cyberthreats. This requires additional research and consultations with experts in the field of cybersecurity, AI, and law to develop effective and balanced legal mechanisms for regulating the use of AI in cybersecurity in Ukraine.

The introduction of AI systems in the cybersecurity of Ukraine’s defence sector is accompanied by a set of legal risks that require a thorough analysis and systematisation. The key categories of legal risks in this context are human rights risks, liability risks, regulatory non-compliance risks, international law risks, and ethical risks. Each of these categories covers a wide range of potential legal issues that require detailed consideration and assessment.

Risks of human rights violations, including the right to privacy, freedom of expression, and non-discrimination, become particularly relevant when AI is used in defence cybersecurity. AI systems, by collecting and analysing large amounts of personal data, may violate the right to privacy guaranteed by Article 8 of the Convention for the Protection of Human Rights [31]. AI algorithms aimed at detecting threats may unduly restrict the freedom of expression protected by Article 10 of the Convention or promote discrimination against certain groups, contrary to Article 14. In this context, the principle of proportionality is of particular significance, as any restriction of rights must be necessary and consistent with a legitimate aim.

The liability risks associated with determining who is liable in case of errors or failures of AI systems pose significant legal challenges. In the context of the defence sector, where the consequences of such mistakes can be critical to national security, this issue is particularly acute. Defining clear boundaries of responsibility for developers, operators, and end users of AI systems is a key task to minimise this risk category. From a legal perspective, this requires the development of special legislation that would consider the specifics of AI and its application in the defence sector. This approach is supported by the European Commission’s recommendations on the legal regulation of AI [32].

Risks of regulatory non-compliance arise from potential conflicts between the operation of AI systems and existing legal regulations. In the defence sector, this problem is compounded by the requirement to follow both national legislation and international standards on cybersecurity and information protection. Particular attention should be paid to the compliance of AI systems with the requirements of the Law of Ukraine No. 2297-6 “On Personal

Data Protection" [32] and the Law of Ukraine No. 3855-12 "On State Secrets" [23]. The legal assessment of these risks points to the need to develop special regulations that will govern the use of AI in the defence sector and define clear requirements for the protection of information and personal data.

International law risks relate to potential violations of international agreements and conventions in the field of cybersecurity and defence. The use of AI in the defence sector may lead to situations where autonomous actions of AI systems potentially violate international norms of cyber warfare or principles of international humanitarian law, in particular the Geneva Conventions and their Additional Protocols. The legal assessment of these risks points to the need to develop international standards and protocols for the use of AI in the military sphere, as well as the significance of including AI provisions in existing international cybersecurity treaties. Ethical risks associated with possible ethical dilemmas in decision-making by AI systems are of particular importance in the context of cybersecurity in the defence sector. Decisions made by AI can have dire consequences for human life and health, as well as for national security in general.

Table 2. Matrix for assessing the legal risks of introducing AI into cybersecurity

Risk category	Risk description	Probability (1-5)	Severity of consequences (1-5)	General risk assessment	Possible measures of protest
Human rights violations	Unlawful restriction of freedom of expression through excessive content filtering	4	5	20	Development of clear filtering criteria, regular audit of the system, and a mechanism for appealing decisions
Risk of liability	Difficulty in identifying the responsible entity in case of false identification of a threat by the AI system	3	4	12	Implementation of a system of shared responsibility, mandatory risk insurance
Regulatory non-compliance	Conflict between AI algorithms and the requirements of personal data protection legislation	5	3	15	Development of special legislation on the use of AI in the defence sector, consultations with legal experts
International law	Potential violation of international cybersecurity agreements due to autonomous actions of an AI system	2	5	10	Implementation of international standards in the field of AI, constant monitoring of compliance with international law
Ethical risks	AI system making decisions that contradict the ethical norms of society	3	4	12	Development of a code of ethics for AI systems, creation of an ethics committee to oversee the implementation of AI

Note: The total risk score in this matrix is calculated as the product of two parameters: Probability of Risk Occurrence and Consequence Severity. Both of these parameters are rated on a scale from 1 to 5, where 1 is the minimum value and 5 is the maximum.
Source: created by the authors.

The developed methodology for legal risk assessment consists of five main stages: risk identification, qualitative risk assessment, quantitative risk assessment, risk ranking, and development of recommendations. The key tool of the methodology is the Matrix for Assessing Legal Risks of AI Implementation in Cybersecurity, which allows visualising and analysing the identified risks (Table 2).

Applying this matrix to the example of assessing the legal risks of implementing an AI system to detect and counter disinformation in the defence sector of Ukraine shows that the most critical risk is the risk of violating human rights, specifically freedom of expression. This underscores the need to strike a balance between national security and the protection of fundamental human rights following the principles set out in the judgements of the European Court of Human Rights (ECtHR). In the case of Big Brother Watch and Others v. the United Kingdom [33], the court emphasised the need to establish clear and predictable rules for mass interception of communications, which directly relates to the use of AI in cybersecurity. Additionally, the Case of Centrum för Rättvisa v. Sweden [34] highlighted the significance of effective supervision and control over mass surveillance systems, which is also a critical aspect of AI implementation in the defence sector.

The legal assessment of the developed methodology for assessing the risks of introducing AI into the cybersecurity of the defence sector shows its potential as a tool for preventive legal regulation. This methodology could become the basis for mandatory legal expertise of AI systems before their introduction into critical infrastructure. From an administrative standpoint, it can be implemented through mandatory certification of AI systems for the defence sector. This will create a legal mechanism to ensure that AI technologies follow regulatory requirements at the development stage. In the field of information law, the methodology can become the basis for the formation of a new category of "information and algorithmic security", which will cover the risks associated with the autonomy of AI systems. From the perspective of constitutional law, its application will help to balance the interests of national security and human rights protection by creating a mechanism for assessing possible violations. In international law, this methodology could become the basis for creating standards for AI risk assessment in the military sphere, helping to harmonise the approaches of different countries to regulating this technology.

An urgent need was identified to adapt Ukraine's national legislation to effectively regulate the use of AI in defence cybersecurity. The rapid development of AI technologies and their implementation in the field of cybersecurity create new challenges for legal regulation. In the Ukrainian context, this problem is particularly acute considering the current geopolitical situation and growing cyberthreats. Effective legal regulation of AI in cybersecurity requires a comprehensive approach that covers both the technical and ethical aspects of the use of these technologies.

The following amendments are proposed to concrete laws and regulations of Ukraine. The Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [19] should be amended to include definitions of "artificial intelligence systems in cybersecurity" and "autonomous cyber defence systems" in Article 1. These definitions should be based on modern international standards, specifically on the recommendations developed by the Organisation for Economic Cooperation and Development [35]. Furthermore, it is proposed to supplement Section II with an article on the specifics of AI application in critical infrastructure cyber defence systems. In terms of the Law of Ukraine No. 2297-6 "On Personal Data Protection" [22], it is proposed to amend Article 6 to define the specifics of personal data processing by AI systems in the context of cybersecurity. It is also recommended that the law be supplemented with a section on the rights of personal data subjects in relation to decisions made by automated AI systems. It is important to ensure human control over automated decision-making systems. The Law of Ukraine No. 2469-8 "On National Security of Ukraine" [21] is proposed to be amended by supplementing Article 1 with the definition of "threat to national security in the field of AI". This definition should consider both the potential risks of AI being used by malicious actors and the risks associated with the insufficient development of AI technologies in Ukraine, which may lead to a technological lag in cybersecurity. It is also recommended to amend Section III to include provisions on the strategy for the development and application of AI in the national security system. This strategy should factor in both the defensive and offensive aspects of using AI in cyberspace.

It is proposed to develop and adopt new regulatory acts, namely the Law of Ukraine "On Regulation of Artificial Intelligence in the Field of National Security and Defence". This law should define key concepts and classify AI systems, establish a legal framework for their development, testing, and implementation in the defence sector, regulate responsibility for decisions made by AI, and prescribe mechanisms for monitoring and auditing AI systems in critical infrastructure. It is also recommended to adopt the Resolution of the Cabinet of Ministers of Ukraine (CMU) "On the Procedure for Certification of Artificial Intelligence Systems for Use in Cybersecurity". This resolution should establish the criteria and procedures for certification, determine the authorised certification body, and regulate the procedures for periodic audits of certified systems. When developing this resolution, it is advisable to consider the EU practices in creating an AI certification system.

To ensure the transparency of AI algorithms in the context of national security, it is proposed to introduce an "explainable AI" system for critical decision-making systems. It is important to emphasise an understanding of the decision-making process of AI systems to ensure trust and accountability. Furthermore, it is recommended to create a register of AI algorithms used in cybersecurity systems of national significance and to establish requirements for documenting the decision-making process of AI systems. To improve the legal protection of critical infrastructure when using AI, it is proposed to develop a methodology for assessing the risks of introducing AI into critical infrastructure protection systems. This methodology should consider both technical and socio-economic aspects of AI implementation. It is also recommended to create a system for early detection and response to anomalies in the operation of AI systems of critical infrastructure and to implement backup control mechanisms in case of failures in the operation of autonomous AI systems.

The proposed amendments to legislation and new regulations should create a system of legal regulation of AI in cybersecurity in Ukraine. Their implementation will increase the efficiency of AI in the defence sector and ensure the protection of citizens' rights and national interests in the digital space. At the same time, the process of adapting legislation should be flexible and accommodate the rapid development of AI technologies. AI regulation should balance innovation and risk mitigation, which is particularly important in the context of national security and cybersecurity.

Discussion

The results of the study of the legal aspects of using AI to ensure cybersecurity of the Ukrainian defence sector have revealed a series of prominent issues and prospects that require detailed analysis and discussion in the context of global trends and research. The identified mismatch between the rapid development of AI technologies and the existing regulatory framework of Ukraine is typical not only for this country but also for many other countries. This is confirmed by the findings of Taddeo et al. [5], who point to the global problem of a "regulatory gap" in the field of AI and cybersecurity. The researchers emphasise the need to develop flexible legal mechanisms capable of adapting to rapid technological changes, which is in line with the conclusions about the need to update Ukrainian legislation. At the same time, the study revealed aspects of this problem specific to Ukraine, specifically, the lack of a legal definition of AI in the context of cybersecurity and the unresolved issues of liability for the actions of autonomous systems. These aspects are particularly important in the context of growing cyberthreats to Ukraine's defence sector.

The proposed methodology for assessing the legal risks of introducing AI into cybersecurity is supported [36], who emphasises the significance of a systematic approach to assessing AI risks in critical infrastructures. The risk assessment matrix, which includes such categories as human rights violations, liability, regulatory non-compliance, international law, and ethical aspects, correlates with the framework proposed by these researchers. However, the study extends this approach by adapting it to the specific needs of the Ukrainian defence sector and focusing on legal aspects. This allows for a more accurate assessment of risks in the context of national security and cybersecurity. The identified risks of human rights violations in the use of AI in cybersecurity, including potential restrictions on freedom of expression and risks of discrimination, are confirmed by Smuha [14]. The researcher emphasises the need for a balance between the efficiency of AI systems and the protection of fundamental rights, which is in line with the recommendations for implementing control and audit mechanisms for AI systems in critical infrastructure. At the same time, the study extends this discussion by examining these risks in the specific context of Ukraine's defence sector, where the balance between national security and human rights is particularly acute.

Cath et al. [37] support the proposed amendments to Ukrainian legislation, specifically the inclusion of definitions of AI and autonomous cyber defence systems in the relevant laws. The researchers emphasise the significance of clear legal definitions for effective regulation of AI in critical sectors. The study develops this idea by proposing concrete wording and mechanisms for their implementation in Ukrainian legislation, which can serve as a model for other countries facing comparable challenges. The identified need for special legislation on the use of AI in the defence sector is in line with the findings of Brockmann et al. [38], who emphasise the need to develop a specific legal framework for the military use of AI. However, the study goes further by proposing a concrete framework for such legislation for Ukraine, including mechanisms for certification and audit of AI systems. This could be an important contribution to the development of international law in the field of regulation of military AI technologies.

Recommendations for the implementation of explainable AI for critical decision-making systems are supported by Robbins [39], who emphasises the importance of algorithm transparency to ensure trust and accountability. The study expands on this concept by proposing concrete mechanisms for its implementation in the context of cybersecurity in Ukraine's defence sector, including the creation of a register of AI algorithms and the establishment of requirements for documenting decision-making. The identified problem of unresolved issues of personal data protection when using AI to analyse cyberthreats is consistent with the findings of Tsamados et al. [40], who emphasise the need to develop special rules for data processing by AI systems in the context of national security.

The proposed concept of "information and algorithmic security" as a new category in information law is supported by Dignum [41], who emphasises the need to expand legal concepts to adequately reflect the reality of AI. The identified need to adapt international law to the challenges of AI in cybersecurity is consistent with the findings of Schmitt [42], who emphasises the need to revise existing international norms in light of latest technologies. The study extends this discussion by proposing specific areas for international cooperation in the field of AI regulation in the defence sector, which could become a valuable contribution of Ukraine to the development of international cybersecurity law.

Perry and Uuk [43] support the recommendations for creating a system for early detection and response to anomalies in the operation of AI systems in critical infrastructure, who emphasise the significance of a proactive approach to AI risk management. The results propose concrete mechanisms for its implementation in the context of cybersecurity of the defence sector of Ukraine. The identified need to balance innovation and risk mitigation in AI regulation is consistent with the findings of Floridi et al. [44], who emphasise the need for "ethical design" of AI systems. The study advances this concept by introducing concrete legal mechanisms to ensure the ethical use of AI in cybersecurity, including the establishment of ethics committees and the development of codes of ethics.

Brundage et al. [45] support the proposals for the introduction of public-private partnership mechanisms in the development of AI for cybersecurity, emphasising the importance of cooperation between the government and the private sector in the development of secure AI systems. The results of the study develop this idea by proposing concrete legal mechanisms for such cooperation in the context of Ukraine's defence sector. This need becomes particularly relevant in the context of Ukraine's Euro-Atlantic integration and the need to harmonise national legislation with EU and NATO standards. These conclusions are confirmed by Ulnicane et al. [46], who analysed trends in international cooperation in the field of AI regulation. Effective regulation of AI in a globalised world requires coordinated efforts of the international community, especially in such sensitive areas as cybersecurity and defence.

Recommendations for the introduction of mandatory legal expertise of AI systems before their introduction into critical infrastructure are supported by Yeung et al. [47], who emphasise the significance of preventive legal regulation of AI. The study proposes concrete mechanisms for such expertise in the context of cybersecurity of the defence sector of Ukraine. The identified need for the development of specialised education and training in the field of legal regulation of AI in cybersecurity is consistent with the findings of Mökander et al. [48], who emphasise the significance of an interdisciplinary approach to AI governance. The study extends this concept by proposing concrete vectors for the development of educational programmes and training in Ukraine.

In addition to these findings, it is worth paying attention to the study by Horowitz et al. [49], which addresses the issue of strategic stability in the context of AI in the defence sector. The researchers emphasise the need to develop international protocols to prevent the escalation of conflicts caused by errors or misinterpretation of AI systems. This study adds an important dimension to the consideration of the legal aspects of the use of AI in cybersecurity, focusing on the geopolitical implications of the introduction of such technologies. Schraagen [50] extends the discussion on the legal regulation of AI in cybersecurity by considering the issue of liability for damage caused by autonomous systems. The researcher proposes an innovative approach to the definition of responsibility, which accommodates the complexity of human-machine interaction in the decision-making process. This study provides more arguments in favour of developing specialised legislation to regulate AI in the defence sector, emphasising the need to consider the unique characteristics of autonomous systems when determining legal liability.

In summary, the findings of the study not only confirm the conclusions of many international experts on the significance of adapting legal regulation to the challenges of AI in cybersecurity, but also expand existing knowledge by offering concrete mechanisms and recommendations for Ukraine. Particularly important is the contribution to the development of a methodology for assessing legal risks of AI in the context of national security and proposals for the adaptation of Ukrainian legislation. These results may be useful not only for Ukraine, but also for other countries facing comparable challenges in regulating AI in the defence sector. At the same time, the study identified a series of issues that require further investigation, including mechanisms for international harmonisation of legal regulation of AI in cybersecurity and the development of effective systems for auditing and controlling AI in critical infrastructures. These areas could form the basis for future research in this important and dynamic area.

Conclusions

This study addressed the critical issue of legal regulation for the use of artificial intelligence (AI) in ensuring cybersecurity within Ukraine's defence sector, presenting a conceptual model tailored to the country's unique challenges. The research revealed significant gaps in Ukrainian legislation, including the absence of definitions and classifications for AI systems, unclear responsibility for autonomous decisions, and the lack of certification standards for cybersecurity-related AI technologies. These gaps pose risks to national security and hinder the efficient integration of advanced technologies. A comparative analysis of international practices, particularly from the USA, EU, UK, and Israel, demonstrated the necessity of adopting specialised legislation. Israel's approach, centred on active defence strategies using AI, proved especially relevant for addressing hybrid threats and information warfare in Ukraine.

The study developed a methodology for assessing the legal risks of AI integration, highlighting the high probability and severe consequences of human rights violations, such as restrictions on freedom of expression. It was recommended that Ukraine amend existing laws and adopt new legislation, including a draft law "On the Regulation of Artificial Intelligence in the Field of National Security and Defence." Additionally, establishing certification and audit mechanisms for AI systems would enhance their reliability and align with international best practices.

These findings have practical implications for strengthening Ukraine's cybersecurity infrastructure, ensuring transparency and accountability in AI applications, and balancing technological advancement with the protection of fundamental rights. The proposed framework not only addresses current legislative deficiencies but also provides a forward-looking strategy for adapting to evolving technologies and security challenges. Further research is required to refine these recommendations and explore international collaboration in regulating AI for cybersecurity.

References

[1] Kovalchuk, O., Banakh, S., Chudyk, N., & Drakokhrust, T. (2024). Machine learning models for judicial information support. Law, Policy and Security, 2(1), 33-45. https://doi.org/10.62566/lps/1.2024.33

[2] Khadzhiradieva, S., Bezverkhniuk, T., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. Social and Legal Studios, 7(3), 245-256. https://doi.org/10.32518/sals3.2024.245

[3] Dashkovska, A. (2022). Administrative and legal status of the national security and defence council of Ukraine as a subject of information security of the state. Law Journal of the National Academy of Internal Affairs, 12(3), 86-96. https://doi.org/10.56215/04221203.86

[4] Aizhan Satayeva, Disclosure in Civil Proceedings in the UK and Kazakhstan: Comparative Analysis, Statute Law Review, Volume 44, Issue 3, December 2023, hmad010, https://doi.org/10.1093/slr/hmad010

[5] Taddeo, M., McCutcheon, T., Floridi, L. 2019. Trusting Artificial Intelligence in Cybersecurity is a Double-Edged Sword. *Nature Machine Intelligence*, 1(12), 557-560. https://doi.org/10.1038/s42256-019-0109-1

[6] Kaushik, K., Khan, A., Kumari, A., Sharma, I., Dubey, R. 2024. Ethical Considerations in AI-Based Cybersecurity. In: K. Kaushik, I. Sharma (Eds.), *Next-Generation Cybersecurity. Blockchain Technologies* (pp. 437-470). Singapore: Springer. https://doi.org/10.1007/978-981-97-1249-6_19

[7] Usman, H., Nawaz, B., Naseer, S. 2023. The Future of State Sovereignty in the Age of Artificial Intelligence. *Journal of Law & Social Studies*, 5(2), 142-152. https://www.advancelrf.org/wp-content/uploads/2023/04/Vol-5-No.-2-1.pdf

[8] Kanellopoulos, A.N. 2024. Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges. *Journal of Politics and Ethics in New Technologies and AI*, 3(1), e35617. https://doi.org/10.12681/jpentai.35617

[9] Kant, N.A. 2022. How Cyber Threat Intelligence (CTI) Ensures Cyber Resilience Using Artificial Intelligence and Machine Learning. In: J.O. Prakash, H.L. Gururaj, M.R. Pooja (Eds.), *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics* (pp. 65-96). Pennsylvania: IGI Global. https://doi.org/10.4018/978-1-6684-3991-3.ch005

[10] Margulies, P. 2020. Autonomous Cyber Capabilities below and above the Use of Force Threshold: Balancing Proportionality and the Need for Speed. *International Law*

Studies, 96, 395-441. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2927&context=ils

[11] Haner, J., Garcia, D. 2019. The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development. *Global Policy*, 10(3), 331-337. https://doi.org/10.1111/1758-5899.12713

[12] Radanliev, P., de Roure, D., Walton, R., van Kleek, M., Montalvo, R.M., Maddox, L.T., Santos, O., Burnap, P., Anthi, E. 2020. Artificial Intelligence and Machine Learning in Dynamic Cyber Risk Analytics at the Edge. *Discover Applied Sciences,* 2, 1773. https://doi.org/10.1007/s42452-020-03559-4

[13] Singh, S., Karimipour, H., HaddadPajouh, H., Dehghantanha, A. 2020. Artificial Intelligence and Security of Industrial Control Systems. In: KK. Choo, A. Dehghantanha (Eds.), *Handbook of Big Data Privacy* (pp. 121-164). Cham: Springer. https://doi.org/10.1007/978-3-030-38557-6_7

[14] Smuha, N.A. 2021. From a 'Race to AI' to a 'Race to AI Regulation' – Regulatory Competition for Artificial Intelligence. *Published in Law, Innovation and Technology*, 13(1). https://dx.doi.org/10.2139/ssrn.3501410

[15] Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P.V., Janssen, M., Jones, P., Kar, A.K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., Medaglia, R., Williams, M.D. 2021. Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy. *International Journal of Information Management*, 57, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

[16] Gillespie, N., Lockey, S., Curtis, C. 2021. *Trust in Artificial Intelligence: A Five Country Study.* Brisbane: University of Queensland, KPMG Australia. https://doi.org/10.14264/e34bfa3

[17] National Artificial Intelligence Initiative Act. 2020. https://www.congress.gov/bill/116th-congress/house-bill/6216

[18] Regulation (EU) No. 2024/1689 of the European Parliament and of the Council "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) No. 2018/858, (EU) No. 2018/1139 and (EU) No. 2019/2144 and Directives No. 2014/90/EU, (EU) 2016/797 and (EU) No. 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[19] Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine". 2017. https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[20] Cybersecurity Strategy of Ukraine. 2021. https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini

[21] Law of Ukraine No. 2469-8 "On National Security of Ukraine". 2018. http://zakon.rada.gov.ua/laws/show/2469-19.

[22] Law of Ukraine No. 2297-6 "On Personal Data Protection". 2010. https://zakon.rada.gov.ua/laws/show/2297-17#Text

[23] Law of Ukraine No. 3855-12 "On State Secrets". 1994. https://zakon.rada.gov.ua/laws/show/3855-12#Text

[24] Policy Paper the UK's International Technology Strategy. 2023. https://www.gov.uk/government/publications/uk-international-technology-strategy/the-uks-international-technology-strategy

[25] National AI Strategy. 2021. https://www.gov.uk/government/publications/national-ai-strategy

[26] Artificial Intelligence Strategy of the German Federal Government. 2020. https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

[27] Estonia's National AI strategy. 2019. https://ai-watch.ec.europa.eu/countries/estonia/estonia-ai-strategy-report_en#ecl-inpage-249

[28] Criminal Code of Ukraine. 2001. https://zakon.rada.gov.ua/laws/show/2341-14#Text

[29] Code of Ukraine "On Administrative Offenses". 1984. https://zakon.rada.gov.ua/laws/show/80731-10

[30] Baranov, O., Kostenko, O., Dubniak, M., Golovko, O. 2024. *Digital Transformations of Society: Problems of Law.* Warsaw: RS Global. https://doi.org/10.31435/rsglobal/057

[31] European Convention on Human Rights. 1950. https://zakon.rada.gov.ua/laws/show/995_004#Text

[32] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[33] Zalnieriute, M. 2022. Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law,* 116(3), 585-592. https://doi.org/10.1017/ajil.2022.35.

[34] Case Of Centrum För Rättvisa v. Sweden. 2021. https://hudoc.echr.coe.int/fre#{%22sort%22:[%22kpdate%20Descending%22],%22itemid%22:[%22001-210078%22]}

[35] OECD. 2019. Recommendation of the Council on Artificial Intelligence. https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf

[36] Artificial Intelligence & Cybersecurity: Balancing Innovation, Execution and Risk. 2021. https://impact.economist.com/perspectives/technology-innovation/artificial-intelligence-cybersecurity-balancing-innovation-execution-and-risk

[37] Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., Floridi, L. 2020. Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach. *Science and Engineering Ethics,* 24(2), 505-528. https://doi.org/10.1007/s11948-017-9901-7

[38] Brockmann, K., Bauer, S., Boulanin, V. 2019. *Bio plus X: Arms Control and the Convergence of Biology and Emerging Technologies.* Stockholm: Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2019-03/sipri2019_bioplusx_0.pdf

[39] Robbins, S. 2020. AI and the Path to Envelopment: Knowledge as a First Step Towards the Responsible Regulation and Use of AI-powered Machines. *AI & Society*, 35(2), 391-400. https://doi.org/10.1007/s00146-019-00891-1

[40] Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., Floridi, L. 2022. The Ethics of Algorithms: Key Problems and Solutions. *AI & Society,* 37(1), 215-230. https://doi.org/10.1007/s00146-021-01154-8

[41] Dignum, V. 2019. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way.* Cham: Springer. https://doi.org/10.1007/978-3-030-30371-6

[42] Schmitt, M.N. 2020. Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention. *International Law Studies,* 96, 549-578. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2932&context=ils

[43] Perry, B., Uuk, R. 2019. AI Governance and the Policymaking Process: Key Considerations for Reducing AI Risk. *Big Data and Cognitive Computing,* 3(2), 26. https://doi.org/10.3390/bdcc3020026

[44] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., Vayena, E. 2018. AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707. https://doi.org/10.1007/s11023-018-9482-5

[45] Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., Yang, J., Toner, H., Fong, R., Maharaj, T., Koh, P.W., Hooker, S., Leung, J., Trask, A., Bluemke, E., Lebensold, J., O'Keefe, C., Koren, M., Ryffel, T., Rubinovitz, JB., Besiroglu, T., Carugati, F., Clark, J., Eckersley, P., de Haas, S., Johnson, M., Laurie, B., Ingerman, A., Krawczuk, I., Askell, M., Cammarota, R., Lohn, A., Krueger, D., Stix, C., Henderson, P., Graham, L., Prunkl, C., Martin, B., Seger, E., Zilberman, N., Héigeartaigh, S.Ó., Kroeger, F., Sastry, G., Kagan, R., Weller, A., Tse, B., Barnes, E., Dafoe, A., Scharre, P., Herbert-Voss, A., Rasser, M., Sodhani, S., Flynn, C., Gilbert, T.K., Dyer, L., Khan, S., Bengio, Y., Anderljung, M. 2020. *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims.* https://arxiv.org/pdf/2004.07213

[46] Ulnicane, I., Knight, W., Leach, T., Stahl, B.C., Wanjiku, W.G. 2022. Governance of Artificial Intelligence: Emerging International Trends and Policy Frames. In: T. Maurizio (Ed.), *The Global Politics of Artificial Intelligence* (pp. 29-55). New York: Chapman and Hall/CRC. https://library.oapen.org/handle/20.500.12657/54691

[47] Yeung, K., Howes, A., Pogrebna, G. 2019. AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing. In: M.D. Dubber, F. Pasquale, S. Das (Eds.), *The Oxford Handbook of Ethics of AI* (pp. 76-106). Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.5

[48] Mökander, J., Axente, M. 2023. Ethics-Based Auditing of Automated Decision-Making Systems: Intervention Points and Policy Implications. *AI & Society*, 38(1), 153-171. https://doi.org/10.1007/s00146-021-01286-x

[49] Horowitz, M., Scharre, P. 2021. AI and International Stability: Risks and Confidence-Building Measures. https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.

[50] Schraagen J.M. 2023. Responsible Use of AI in Military Systems: Prospects and Challenges. *Ergonomic*s, 66(11), 1719-1729. https://doi.org/10.1080/00140139.2023.2278394