

DOI <https://doi.org/10.32353/acfs.9.2024.08>
UDC 342.951:004.9

Dmytro Kaliuzhnyi

Applicant for the third level academic education (PhD in Law),
Department of Law, Faculty of Humanities and Law,
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine
ORCID: <https://orcid.org/0009-0006-1709-8405>
e-mail: dmitrijkoluznyj555@gmail.com

Legal Grounds For Artificial Intelligence Use In Law Enforcement: International And Foreign Experience

Artificial intelligence (AI) has become an integral part of modern law enforcement officers, providing them with unprecedented capabilities in crime prevention, investigation and analysis. AI technologies, such as biometrics and facial recognition systems, police activity forecasting algorithms, and AI-assisted X-ray interpretation, are transforming traditional methods of law enforcement officers' work in order to increase their efficiency and effectiveness. However, along with potential advantages, the widespread adoption of AI in law enforcement raises ethical, legal, and social issues necessitating increased focus from government legislative, executive, and human rights authorities.

The Article Purpose is to study regulatory and legal grounds for state regulation of AI technologies use in human rights protection activities in developed countries. Relying on the analysis of international and foreign experience, identify directions for further development of a corresponding Ukrainian legislation.

Methodology: The main methodological approach applied is a regulatory approach. The paper will be based on the qualitative method consisting in the collection and processing of data to compare and interpret provisions or policies that support the implementation of AI in public life with adherence to the fundamental rights and freedoms, as well as ensuring safety and non-discrimination guarantees. The following methods have been applied in this article: research method, descriptive method, comparative and analytical method, interpretive analysis method, and illustrative method.

Conclusions. Based on the analysis of regulations and legislative experience of the EU, the USA, and other developed countries involved in legal regulation of AI application, the author reveals trends and principles of AI technologies use in law enforcement. Namely: 1. Absolute majority of acts are aimed at protecting fundamental human rights and overall democratic functioning of society. 2. The principles of accountability, transparency and justice are found in nearly all well-known and common AI governance structures. 3. Singling out different forms of artificial intelligence. Most legal regulations distinguish between different types of AI systems depending on the risks they pose, the context in which they are used, or the specific type of system they create.

Key words: law enforcement, law enforcement officers, artificial intelligence, application of information technology in law enforcement, foreign experience, legal regulation.

Research Problem Formulation. In recent years, the activities of law enforcement officers in Ukraine have been hindered by both internal socio-political factors and external threats. Despite the hostilities, Ukraine has been maintaining its integration into the European and global information society.



Dmytro Kaliuzhnyi

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclaimer

The funder had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Contributors

The author contributed solely to the intellectual discussion underlying this paper, case-law exploration, writing and editing, and accept responsibility for the content and interpretation.

Declaration of Competing Interest

The author declare that they have no conflict of interest.



Дмитро Калужний

**ПРАВОВІ ОСНОВИ
ЗАСТОСУВАННЯ ШТУЧНОГО
ІНТЕЛЕКТУ У ДІЯЛЬНОСТІ
ПРАВООХОРОННИХ
ОРГАНІВ: МІЖНАРОДНИЙ І
ЗАРУБІЖНИЙ ДОСВІД**

Штучний інтелект (ШІ) став невід'ємною частиною сучасних правоохоронних органів, пропонуючи їм безпрецедентні можливості в запобіганні, розслідуванні та аналізі злочинів. Технології штучного інтелекту, такі як: біометрія і системи розпізнавання обличчя, алгоритми прогнозування діяльності поліції, рентгенівське бачення ШІ, змінюють традиційні методи роботи правоохоронців в напрямку підвищення її ефективності та результативності. Однак, поряд із потенційними перевагами, широке впровадження ШІ в правоохоронних органах спричиняє етичні, юридичні та соціальні проблеми, які потребують підвищеної уваги з боку державних законодавчих, виконавчих і правозахисних органів.

Метою статті є дослідження нормативно-правових засад державного регулювання використання технологій ШІ у правоохоронній діяльності в розвинутих країнах світу. На основі аналізу міжнародного та зарубіжного досвіду виокремити напрями подальшого розвитку відповідного законодавства в Україні.

Методологія: Основним застосованим методичним підходом є нормативний підхід. Стаття базуватиметься на якісному методі, який полягає у зборі та обробці даних для порівняння та інтерпретації положень або політики, що забезпечують впровадження штучного інтелекту у суспільне життя із дотриманням основних прав і свобод, а також забезпечення безпеки і гарантій недискримінації. У цій статті застосовані такі методи: метод дослідження, описовий метод, порівняльно-аналітичний метод, метод інтерпретаційного аналізу та ілюстративний метод.

Висновки. На підставі аналізу нормативних актів і законодавчого досвіду ЄС, США і інших розвинених країн світу в сфері правового регулювання застосування ШІ автор виділяє тенденції і принципи використання технологій ШІ у правоохоронній діяльності. А

Thus, regional cooperation in the context of Ukraine's European integration, as well as joint projects with international institutions, emphasize the importance of introducing state-of-the-art information and communications technologies and artificial intelligence technologies into law enforcement.

Digital technologies are gradually penetrating into various areas of our lives, year after year. They are a crucial factor in the development of modern human society, affecting not only such traditional areas as medicine, production and education, but also legal relations. In Ukraine, on March ¹, 2023, the new Law of Ukraine On the National Informatization Program entered into force, which main task is the development, implementation and application of information and communications technologies in public administration, local self-government and public life. And law enforcement officers are defined as one of its subjects ¹. Scientific literature defines the content of digitalization process in society as "legal, political, economic, cultural, social and political changes conditioned by the use of digital tools and technologies" ². At the same time, the Concept of Artificial Intelligence Development in Ukraine states that artificial intelligence technologies are considered as part of information technologies. According to the document, Ukraine, which is a member of the Ad Hoc Committee on Artificial Intelligence at the Council of Europe, joined the Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449) in October 2019. Accordingly, one of the priority avenues and principal tasks for the development of artificial intelligence technologies is to observe the rights and legitimate interests of individuals and legal entities, build a competitive national economy, and improve public administration ³ system. In this respect, it is of particular importance to study international and foreign experience in this area and consider strengthening information and analytical support for law enforcement in Ukraine.

Analysis of Essential Research and Publications. The issues of information support and AI implementation in the activities of law enforcement officers were addressed by I. V. Aristova, K. I. Bieliakov, R. A. Kaliuzhnyi, V. A. Lypkan, O. M. Podoliak et al. Particular issues related to legal regulation of ICT are covered in research papers by L. Karl Brantinh, M. Berdzhes, M. D. Vasylenko, S. M. Husarov, O. H. Zabolotnyi, O. M. Okhotnikov, I. Katerynychuk. Simultaneously, the issue of studying international and foreign experience of utilizing information technologies in the activities of law enforcement officers remains out of focus. The Article Purpose is to study the regulatory and legal framework for regulating the use of AI technologies in human rights activities by governments in developed countries. Stemming from the analysis of international and foreign experience, the author identifies areas for further development of a relevant Ukrainian legislation.

Main Content Presentation. Today, artificial intelligence (AI) is becoming an increasingly popular tool in the activities of law enforcement officers and other state institutions. Despite the fact that technologies significantly increase the efficiency of law enforcement practice, it is worth noting that this progress also requires determining the range of limitations and expectations. This is because AI not only fundamentally alters the approach to crime prevention, investigation and prosecution, but also leads to the emergence of a number of legal and ethical issues. For example, artificial intelligence algorithms can analyze large volumes of data and identify patterns that

¹ Про Національну програму інформатизації: Закон України від 01.12.2022 №2807-IX Верховна Рада України. URL: // <https://zakon.rada.gov.ua/laws/show/2807-20#Text>

² Razmetaeva Yu, Barabash Yu, Lukianov D 'The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice' 2022 3(15) Access to Justice in Eastern Europe 41-56. URL: https://ajee-journal.com/upload/attaches/att_1660480856.pdf

³ Концепція розвитку штучного інтелекту в Україні. Схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-п. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>

analysts might not even notice. This has already led to the development of smart policing, which uses artificial intelligence to identify areas where crime is likely to occur and allocate resources accordingly. Artificial intelligence has the potential to significantly affect the content of law enforcement officers' official duties, and to adjust the requirements for their professional skills and work duties 4. Thus, AI is becoming increasingly relevant in law enforcement, enhancing operational efficiency and facilitating better integration and implementation of new devices and technologies. However, there are some challenges and ethical reflections. One of the main reasons for this concern is the possibility of bias in AI algorithms, resulting in discrimination. Another concern is the lack of transparency within AI algorithms. It may be a struggle to understand how the algorithm arrived at a particular decision, making it difficult to appeal against or accept that decision. Finally, there are concerns about the impact of AI on human decision-making. There is a risk that human judgment will be replaced by automated decision-making since artificial intelligence is becoming increasingly prevalent in criminal and administrative proceedings. This could seriously undermine fairness and transparency within criminal justice system.

Currently, the safety and security of citizens and the state as a whole directly depends on information support of law enforcement officers in Ukraine. Problems stemming from armed aggression against our country, information warfare, and subversive activities of the enemy on the territory of Ukraine are becoming of paramount importance. We believe that it is entirely fair to say that international police cooperation should be viewed as one of the components of governments' interaction in the fight against crime, which itself is an important part of international relations. This involves integrating domestic information and analytical systems into international systems and improving these systems according to the technological level required by developed countries, especially the European Union 5.

On December 4, 2009, in Kyiv, Ukraine signed an Agreement with the European Police Office on Strategic Cooperation, which was ratified on October 5, 2010. The purpose of this Agreement was to strengthen cooperation between the European Union Member States, acting through Europol, and Ukraine in prevention, detection, suppression and investigation of serious forms of international crime, specifically through the exchange of strategic and technical information 6. The document expired in 2017 due to the signing of a new agreement On Operational and Strategic Cooperation emphasizing protection of personal data during their transfer or processing. Moreover, Article 4 of the specified Agreement states that "the cooperation may, additional to the exchange of information, in accordance with the tasks of Europol as outlined in the Europol Council Decision, in particular include the exchange of specialist knowledge, general situation reports, results of strategic analysis, information on criminal investigation procedures, information on crime prevention methods, participation in training activities as well as providing advice and support in individual criminal investigations 7.

саве: 1. Абсолютна більшість активів направлені на захист фундаментальних права людини, а також загальне демократичне функціонування суспільства. 2. Принципи підзвітності, прозорості та справедливості присутні практично в усіх добре відомих і загальноприйнятих структурах управління ШІ. 3. Виділення різних форм штучного інтелекту. Більшість нормативних актів розрізняє різні типи систем штучного інтелекту в залежності від ризиків, які вони становлять, контекст, у якому вони використовуються, або певний тип системи, яку вони створюють.

Ключові слова: правоохоронна діяльність, правоохоронні органи, штучний інтелект, застосування інформаційних технологій в правоохоронній діяльності, зарубіжний досвід, правове регулювання.

Dmytro Kaliuzhnyi

Rechtliche Grundlagen für den Einsatz künstlicher Intelligenz in der Strafverfolgung: Internationale und ausländische Erfahrungen

Künstliche Intelligenz (KI) ist zu einem integralen Bestandteil moderner Strafverfolgungsbeamter geworden und bietet ihnen beispiellose Möglichkeiten bei der Kriminalprävention, -ermittlung und -analyse. KI-Technologien wie Biometrie- und Gesichtserkennungssysteme, Algorithmen zur Prognose polizeilicher Aktivitäten und KI-gestützte Röntgeninterpretation verändern die traditionellen Methoden der Arbeit von Strafverfolgungsbeamten, um ihre Effizienz und Effektivität zu steigern. Neben potenziellen Vorteilen wirft die weit verbreitete Einführung von KI in der Strafverfolgung jedoch ethische, rechtliche und soziale Fragen auf, die eine verstärkte Aufmerksamkeit der staatlichen Legislative, Exekutive und Menschenrechtsbehörden erfordern.

Der Zweck des Artikels besteht darin, die regulatorischen und rechtlichen Grundlagen für die staatliche Regulierung des Einsatzes von KI-Technologien bei Menschenrechtsschutzaktivitäten in Industrieländern zu untersuchen. Auf der Grundlage der Analyse internationaler und ausländischer Erfahrungen

⁴ Гуцу С.Ф. Упровадження штучного інтелекту в трудові відносини: перспективи правового регулювання. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 2 (50) 2021. С. 87-92. URL: <http://socio-journal.kpi.kiev.ua/archive/2021/2/16.pdf>

⁵ Іван Катеринчук Міжнародний та зарубіжний досвід застосування інформаційних технологій у діяльності правоохоронних органів. Національний юридичний журнал: теорія та практика. Червень. 2015. С. 22-26. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/efd04dce-59c5-49cd-b868-a14881450289/content>

⁶ Угода між Україною та Європейським поліцейським офісом про стратегічне співробітництво: Закон України від 5 жовтня 2010 року № 2576-VI. Офіційний вісник України. 2010. № 96/№ 84. Ст. 2934/3432. URL: https://zakon.rada.gov.ua/laws/show/994_954#Text

⁷ УГОДА між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво, ратифікована Законом від 12.07.2017 № 2129-VIII. Офіційний вісник України. 08.08.2017 2017 р., № 62, / № 71, 2017, ст. 2192. URL: https://zakon.rada.gov.ua/laws/show/984_001-16#Text

sollen Richtungen für die weitere Entwicklung einer entsprechenden ukrainischen Gesetzgebung ermittelt werden.

Methodik: Der wichtigste angewandte methodische Ansatz ist ein regulatorischer Ansatz. Das Dokument basiert auf der qualitativen Methode, bei der Daten erhoben und verarbeitet werden, um Bestimmungen oder Richtlinien zu vergleichen und zu interpretieren, die die Implementierung von KI im öffentlichen Leben unter Einhaltung der Grundrechte und -freiheiten sowie der Gewährleistung von Sicherheit und Nichtdiskriminierungsgarantien unterstützen. In diesem Artikel wurden die folgenden Methoden angewendet: Forschungsmethode, beschreibende Methode, vergleichende und analytische Methode, interpretierende Analyse-methode und illustrative Methode.

Schlussfolgerungen. Basierend auf der Analyse von Vorschriften und Gesetzgebungserfahrungen der EU, der USA und anderer entwickelter Länder, die an der gesetzlichen Regulierung der KI-Anwendung beteiligt sind, zeigt der Autor Trends und Prinzipien der Verwendung von KI-Technologien in der Strafverfolgung auf. Nämlich: 1. Die absolute Mehrheit der Gesetze zielt auf den Schutz grundlegender Menschenrechte und des allgemeinen demokratischen Funktionierens der Gesellschaft ab. 2. Die Prinzipien der Rechenschaftspflicht, Transparenz und Gerechtigkeit finden sich in fast allen bekannten und gängigen KI-Governance-Strukturen. 3. Hervorhebung verschiedener Formen künstlicher Intelligenz. Die meisten gesetzlichen Vorschriften unterscheiden zwischen verschiedenen Arten von KI-Systemen, je nach den Risiken, die sie bergen, dem Kontext, in dem sie verwendet werden, oder der spezifischen Art des Systems, das sie erstellen.

Schlüsselwörter: Strafverfolgung, Strafverfolgungsbeamte, künstliche Intelligenz, Anwendung von Informationstechnologie in der Strafverfolgung, ausländische Erfahrung, gesetzliche Regulierung.

The European Union Member States have organized a unified automated system of criminal records within Europol, which has been in operation since 2002. The comprehensive information and analysis system TECS (The Europol Computer System) has, in addition to the AIS itself, the following principal components: an analysis center and an index subsystem. The TECS computer system allows the simultaneous processing and analysis of almost one million records. All information in the system is provided directly by the EU Member States. Each country has its own representative organization in The Hague, the so-called ELOS. Only these organizations can access national databases.

As a rule, information systems of the European Union countries are created at the national level and provide strategic analysis of data on the functioning of criminal groups. At the central level, generalized records of criminals and their actions are kept, legislative proposals for governing criminal police work are prepared, and contacts with Interpol are maintained. Such a distribution of powers makes it possible to better direct and coordinate efforts, taking into account expansion of interregional and international contacts as well as migration of organized criminals, ensuring a greater degree of secrecy, while representatives of criminal circles significantly influence political, economic and often law enforcement structures at the local level, especially in small towns.

In 2004, the European Union (EU) established the European Union Agency for Cybersecurity (ENISA) ⁸. ENISA is an expert examination center for cybersecurity in Europe. It cooperates closely with EU member states and the private sector to promote “the development of a [network and information security (NIS)] culture in society and to raise awareness of NIS” ⁹. ISACA (Information Systems Audit and Control Association) believes that the framework for certifying the cybersecurity of ICT products and services should be regional rather than national, and should use existing global standards and best practices. What is more, in order to avoid new vulnerabilities, it must guarantee that cybersecurity is not ignored at the beginning of the design process when developing products and services. Finally, the EU has recognized that addressing the cybersecurity skills gap is a serious issue, and ISACA strongly supports the call for industry to enhance cybersecurity training for organizations and staff.

In December 2018, Council of Europe European Commission for the Efficiency of Justice (CEPEJ) approved European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. The main goal of the Charter is to improve the efficiency and quality of justice through the processing of court decisions and data by algorithms while respecting the fundamental rights and freedoms guaranteed, in particular, by the ECHR and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Among other things, the Charter defines the basic principles of using artificial intelligence in justice administration. Namely: 1) Principle of respect for fundamental rights: ensure that the implementation of artificial intelligence tools and services are compatible with fundamental rights; 2) Principle of non-discrimination: prevent the development or intensification of any discrimination between individuals or groups of individuals; 3) Principle of quality and security: with regard to the processing of judicial decisions and data in a secure technological environment; 4) Principle of

⁸ European Union Agency for Network and Information Security (ENISA), ‘ENISA: 15 years of building cybersecurity bridges together’, Press release, 20 March 2019. URL: <https://www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together>

⁹ ENISA, About ENISA. URL: <https://www.enisa.europa.eu/about-enisa>

transparency; 5) Principle of impartiality 6) Principle of fairness; 7) Principle “under user control”¹⁰.

In 2021, the increased productivity and widespread availability of artificial intelligence led to the development of a Draft Proposal of the European Parliament and of the Council for a regulation laying down harmonized rules on artificial intelligence, which was adopted by the European Parliament on March 13, 2024 (the AI Act). This Law is intended to be part of a broader AI package that would encompass additional policy measures to support the development of trustworthy AI. The AI Law aims to create a long-term legal framework for AI use. Today, the EU's Artificial Intelligence Act is the world's most comprehensive risk-based, innovation-driven artificial intelligence legislation. It is unique for many reasons:

- offers a multi-level risk classification structure for AI systems;
- aims to standardize artificial intelligence legislation in the EU; and to establish artificial intelligence governing bodies;
- promotes human-centered and trustworthy AI innovation, while preserving fundamental rights and democratic values;
- fosters international cooperation and ensures that AI systems can be safely tested and verified before deployment.

The EU's Artificial Intelligence Act classifies AI systems based on a risk-based approach and sets out four categories of risk: unacceptable risk, high risk, limited risk, and minimal or no risk.

Unacceptable risk AI systems are systems considered a threat to people and will be banned. They include: artificial intelligence systems manipulating human behavior to circumvent the user's free will (e.g., subliminal methods or exploitation of vulnerable groups); judging or classifying individuals based on their behavior; biometric identification and categorization of people in real-time in public places (with certain exceptions).

High risk includes AI systems used in critical areas of life. For example, it can be applied for remote real-time biometrics and post-identification of individuals; as a polygraph in order to help law enforcement officers identify the emotional condition of an individual; and for assessing the reliability of evidence in a criminal proceeding, etc.

Limited risk. AI systems that are subject to transparency obligations fall into this category. For example, chatbots must be designed so that users know they are interacting with a machine.

Minimal risk. Artificial intelligence applications such as video games or spam filters are considered minimal risk and can be freely developed and used within the EU¹¹.

Article 5 of the Law sets forth that the use of “real-time” remote biometric identification systems by law enforcement agencies is usually prohibited, except in exhaustively listed and narrowly defined situations. For example, “real-time” video surveillance may be deployed only if strict security measures are followed, for example, its use is limited in terms of time and geography and can only be allowed after obtaining special preliminary judicial or administrative permission. Such uses may include, for example, targeted searches: (i) the targeted search for specific victims of abduction or human trafficking; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or (iii) the localisation or identification of a person suspected of having committed a criminal offence¹². Also, other high-

Dmytro Kaliuzhnyi

FONDEMENTS JURIDIQUES DE L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE DANS LES FORCES DE L'ORDRE : EXPÉRIENCE INTERNATIONALE ET ÉTRANGÈRE

L'intelligence artificielle (IA) fait désormais partie intégrante des forces de l'ordre modernes, leur offrant des capacités sans précédent en matière de prévention, d'enquête et d'analyse de la criminalité. Les technologies d'IA, telles que les systèmes de biométrie et de reconnaissance faciale, les algorithmes de prévision des activités de la police et l'interprétation des rayons X assistée par l'IA, transforment les méthodes traditionnelles de travail des agents chargés de l'application des lois afin d'accroître leur efficacité et leur efficacité. Cependant, outre les avantages potentiels, l'adoption généralisée de l'IA dans les forces de l'ordre soulève des problèmes éthiques, juridiques et sociaux qui nécessitent une attention accrue de la part des autorités législatives, exécutives et des droits de l'homme.

L'objectif de l'article est d'étudier les fondements réglementaires et juridiques de la réglementation étatique de l'utilisation des technologies d'IA dans les activités de protection des droits de l'homme dans les pays développés. En s'appuyant sur l'analyse de l'expérience internationale et étrangère, identifier les orientations pour le développement ultérieur d'une législation ukrainienne correspondante.

Méthodologie : La principale approche méthodologique appliquée est une approche réglementaire. Le document sera basé sur la méthode qualitative consistant en la collecte et le traitement de données pour comparer et interpréter les dispositions ou politiques qui soutiennent la mise en œuvre de l'IA dans la vie publique dans le respect des droits et libertés fondamentaux, ainsi que pour garantir la sécurité et la non-violation, garanties contre la discrimination. Les méthodes suivantes ont été appliquées dans cet article : méthode de recherche, méthode descriptive, méthode comparative et analytique, méthode d'analyse interprétative et méthode illustrative.

Conclusions. Sur la base de l'analyse des réglementations et de l'expérience législative de l'UE, des États-Unis et d'autres

¹⁰ European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. European commission for the efficiency of justice (CEPEJ). Strasbourg, 3-4 December 2018. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

¹¹ Ігор Реутов Правове регулювання шпунтового інтелекту: міжнародний досвід та українські перспективи. URL: <https://pravo.ua/pravove-rehuliuвання-shtuchnoho-intelektu-mizhnarodnyi-dosvid-ta-ukrainski-perspektyvy/>

¹² Tancrede Montagne Overview of the AI Act, the first ever legal framework on AI. 26. March 2024. URL: <https://paytechlaw.com/en/overview-of-the-ai-act-the-first-ever-legal-framework-on-ai/>

pays développés impliqués dans la réglementation juridique des applications de l'IA, l'auteur révèle les tendances et les principes de l'utilisation des technologies de l'IA dans l'application de la loi. À savoir : 1. La majorité absolue des actes visent à protéger les droits humains fondamentaux et le fonctionnement démocratique global de la société. 2. Les principes de responsabilité, de transparence et de justice se retrouvent dans presque toutes les structures de gouvernance de l'IA bien connues et courantes. 3. Distinguer différentes formes d'intelligence artificielle. La plupart des réglementations juridiques distinguent différents types de systèmes d'IA en fonction des risques qu'ils présentent, du contexte dans lequel ils sont utilisés ou du type spécifique de système qu'ils créent.

Mots clés : forces de l'ordre, agents chargés de l'application des lois, intelligence artificielle, application des technologies de l'information aux forces de l'ordre, expérience étrangère, réglementation juridique.

Dmytro Kaliuzhnyi

**PODSTAWY PRAWNE
WYKORZYSTANIA
SZTUCZNEJ INTELIGENCJI
W EGZEKWOWANIU
PRAWA: DOŚWIADCZENIA
MIĘDZYNARODOWE I
ZAGRANICZNE**

Sztuczna inteligencja (AI) stała się integralną częścią współczesnych funkcjonariuszy organów ścigania, zapewniając im niespotykane dotychczas możliwości zapobiegania przestępstwom, prowadzenia dochodzeń i analiz. Technologie sztucznej inteligencji, takie jak systemy biometryczne i rozpoznawania twarzy, algorytmy prognozowania działań policji czy interpretacja zdjęć rentgenowskich wspomagana sztuczną inteligencją, przekształcają tradycyjne metody pracy funkcjonariuszy organów ścigania w celu zwiększenia ich wydajności i efektywności. Jednak oprócz potencjalnych korzyści powszechne przyjęcie sztucznej inteligencji w egzekwowaniu prawa rodzi kwestie etyczne, prawne i społeczne, wymagające większego skupienia się na rządowych organach ustawodawczych, wykonawczych i zajmujących się prawami człowieka.

Celem artykułu jest zbadanie podstaw regulacyjnych i

risk AI systems are subject to clear obligations due to their significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law. Examples of high-risk AI uses include critical infrastructure, education and vocational training, employment, essential private and public services (e.g., healthcare, banking), certain law enforcement systems, migration and border control management, administration of justice and democratic processes (e.g., influencing elections). Such systems should assess and mitigate risks, keep logs of use, be transparent and accurate, and provide human oversight. Citizens will have the right to file complaints against AI systems and receive explanations regarding decisions based on high-risk AI systems affecting their rights¹³. AI systems whose intended purpose, as defined by the provider, is law enforcement or the administration of justice, are classified as high-risk under Annex III of the Law. As such, they are subject to essential requirements (risk management, testing, data governance, technical documentation, transparency, human oversight, accuracy, robustness and cybersecurity) and to obligations (such as quality management systems, technical documentation, conformity assessment, corrective actions, duty of information, obligations of importers and distributors) as well as standards and conformity assessment¹⁴.

At the European level, the AI Act establishes the European Artificial Intelligence Board (EAIB). Similar to existing European agencies, such as ESMA, the EAIB is empowered to facilitate consistency and coordination between European national competent authorities as regards the implementation of this Act, and shall advise and assist the Commission and national supervisory authorities in analyzing and responding to emerging AI issues.

Recognizing the new rules for General Purpose AI (GPAI) models and the critical need for their implementation at the EU level, the Commission has established an AI Office to oversee these cutting-edge AI models, promote the development of testing standards and practices, and ensure that common rules are implemented across Member States. A scientific panel of independent experts will advise the European AI Office about GPAI models by contributing to the development of methodologies for evaluating the capabilities of foundation models, advising on the designation and the emergence of high impact foundation models, and monitoring possible material safety risks related to foundation models.

The AI Board, which would comprise member states' representatives, will remain as a coordination platform and an advisory body to the Commission and will give an important role to Member States on the implementation of the regulation, including the design of codes of practice for foundation models. Finally, an advisory forum for stakeholders, such as industry representatives, SMEs, start-ups, civil society, and academia, will be set up to provide technical expertise to the AI Board¹⁵.

Therefore, the AI Law seeks to create a long-term legal basis for artificial intelligence use. The goals of the Law on Artificial Intelligence are to protect fundamental rights, harmonize the legal environment for artificial intelligence

¹³ Олександра Кознова Європарламент ухвалив Закон про штучний інтелект. URL: https://biz.ligazakon.net/news/226272_vroparlament-ukhvaliv-zakon-pro-shtuchniy-ntelekt

¹⁴ Пропозиція щодо Регламенту Європейського Парламенту та Ради, що встановлює гармонізовані правила щодо штучного інтелекту - Відповідність правових основ статей 114 і 16 ДФЕС щодо положень, що застосовуються до правоохоронних і судових органів (документ Ради 12302/22) , LIMITE, 12 вересня 2022 р., pdf). Brussels, 12 September 2022. URL: <https://www.statewatch.org/media/3510/eu-council-ai-act-law-enforcement-legal-basis-cls-12302-22.pdf>

¹⁵ Стимулювання інновацій та впровадження штучного інтелекту в Європі. URL: <https://finap.com.ua/stymuluvannya-innovatsij-ta-vprovadzhennya-shtuchnogo-intelektu-v-eyevropi/>



at the European level, and determine legal grounds for AI use in law enforcement.

International cooperation in the field of AI will expand and continue, in particular, the US regulatory developments in the field of AI are of the greatest interest. In October 2022, the Office of Science and Technology Policy of the White House published the Blueprint for an AI Bill of Rights¹⁶. The Blueprint aims to protect and preserve fundamental rights of US citizens in light of the progress made worldwide in artificial intelligence. The main purpose of the Blueprint for an AI Bill of Rights is to ensure that the structure and functions of US democracy remain robust, resilient, and effective in an AI-driven future. In this regard, the initiative includes a set of five broad principles, including Safe and Effective Systems, Algorithmic Discrimination, Data Privacy, Notice and Explanations, and Human Alternatives, Consideration and Fallback. The document serves as a significant legal framework for the activities of government authorities, the police and the judiciary in protecting the rights of citizens in the field of AI.

On October 30, 2023, the US President signed the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The document is about introducing new standards for AI security and safety, protecting privacy, promoting fairness and civil rights, safeguarding consumer and worker rights, and fostering innovation and competition: "(f) Americans' privacy and civil liberties must be protected as AI continues advancing. Artificial Intelligence is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires. Artificial Intelligence's capabilities in these areas can increase the risk that personal data could be exploited and exposed. To combat this risk, the Federal Government will ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks. Agencies shall use available policy and technical tools, including privacy-enhancing technologies (PETs) where appropriate, to protect privacy and to combat the broader legal and societal risks — including the chilling of First Amendment rights — that result from the improper collection and use of people's data"¹⁷. The Order also sets forth that irresponsible use could exacerbate discrimination, bias, and other abuses in the areas of justice, health care, and housing. To ensure that AI promotes justice and civil rights, the Order envisages:

- providing guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems;
- consider providing, as appropriate and consistent with applicable law, guidance, technical assistance, and training to State, local, Tribal, and territorial investigators and prosecutors on best practices for investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI;
- ensuring justice throughout the criminal justice system by developing best practices for the use of AI in sentencing, parole and probation, pretrial release, pretrial detention, etc.¹⁸.

From our perspective, a landmark innovation in the specified document, which must be taken into account by the Ukrainian legislator, is the mandate

prawnych państwowych regulacji dotyczących wykorzystania technologii AI w działaniach na rzecz ochrony praw człowieka w krajach rozwiniętych. Opierając się na analizie doświadczeń międzynarodowych i zagranicznych, określić kierunki dalszego rozwoju odpowiedniego ustawodawstwa ukraińskiego.

Metodologia: Głównym stosowanym podejściem metodologicznym jest podejście regulacyjne. Artykuł będzie oparty na metodzie jakościowej polegającej na gromadzeniu i przetwarzaniu danych w celu porównania i interpretacji przepisów lub polityk wspierających wdrażanie AI w życiu publicznym z poszanowaniem podstawowych praw i wolności, a także zapewnieniem bezpieczeństwa i nienaruszalności gwarancji dyskryminacji. W artykule zastosowano następujące metody: metodę badawczą, metodę opisową, metodę porównawczą i analityczną, metodę analizy interpretacyjnej oraz metodę ilustracyjną.

Wnioski. Na podstawie analizy przepisów i doświadczeń legislacyjnych UE, USA i innych krajów rozwiniętych zajmujących się regulacjami prawnymi zastosowania AI, autor ukazuje trendy i zasady wykorzystania technologii AI w egzekwowaniu prawa. Mianowicie:

1. Zdecydowana większość ustaw ma na celu ochronę podstawowych praw człowieka i ogólnodemokratycznego funkcjonowania społeczeństwa.
2. Zasady odpowiedzialności, przejrzystości i sprawiedliwości można znaleźć w prawie wszystkich dobrze znanych i powszechnych strukturach zarządzania sztuczną inteligencją.
3. Wyróżnienie różnych form sztucznej inteligencji. Większość regulacji prawnych rozróżnia różne typy systemów sztucznej inteligencji w zależności od stwarzanych przez nie zagrożeń, kontekstu, w jakim są wykorzystywane, czy też konkretnego typu tworzonego przez nie systemu.

Słowa kluczowe: egzekwowanie prawa, funkcjonariusze organów ścigania, sztuczna inteligencja, zastosowanie technologii informatycznych w egzekwowaniu prawa, doświadczenia zagraniczne, regulacje prawne.

¹⁶ Blueprint for an AI Bill of Rights. The White House. URL: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

¹⁷ Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. THE WHITE HOUSE, October 30, 2023. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/?utm_source=link

¹⁸ Денис Красніков. Новий указ Президента Байдена про штучний інтелект: більше обмежень чи стимулювання розвитку. 15.11.2023. URL: <https://www.ukrinform.ua/rubric-technology/3787099-novij-ukaz-prezidenta-bajdena-pro-stucnij-intelekt-bilse-obmezen-ci-stimuluvanna-rozvitku.html>

to government authorities to develop a system of standards, tools and tests that would ensure safety/security and robustness of AI systems.

Despite the fact that the EU and the US are regional leaders in the field of AI regulation, the first country in the world to create a National AI Strategy at the governmental level was Canada (the Pan-Canadian AI Strategy was released in 2017). This strategy is a five-year plan for funding research and developing a skilled talent pool for this industry. What is more, the country is a co-founder of the Global Partnership on Artificial Intelligence (GPAI). In 2019, the Government of Canada's AI Advisory Council was established to further develop the Pan-Canadian AI Strategy provisions. Canada has proposed the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27¹⁹, the Digital Charter Implementation Act (2022). The suggested Law provides the basis for responsible design, development and deployment of AI systems, guarantees safety/security and non-discrimination of artificial intelligence systems.

Similar to the EU AI Act, Canada's Bill C-27 also defines classes of AI systems that are considered high-impact systems. In particular, they are as follows:

Court or administrative body decision-making: This class involves AI systems used by courts or administrative bodies for decision-making with respect to individuals in legal or administrative proceedings. The goal is to prevent biases in these systems, which could have severe consequences for individuals' rights and access to justice.

Law enforcement: This class covers AI systems used by peace officers for law enforcement purposes. Given the significant impact of policing on individuals and communities, the Government highlights that there is an interest in ensuring these systems are non-discriminatory, safe, and effective.

When adding new classes of high-impact systems, the Government (Governor-in-Council) must consider the severity and extent of potential adverse impacts, including on human rights and social harms²⁰.

The experience of Great Britain actively deploying AI in police officers' work should not be disregarded. For example, this technology makes use of the police archive and studies the decisions made by police officers in similar cases within administrative proceedings during a certain period of time. Later, it assesses risks, considering various factors, and connects them with similar offenses. This contributes to the evaluation of evidence by the police or court authorities and the adoption of a procedural decision on a case. At the same time, police regularly audit AI operation and reliability of its conclusions. On September 28, 2023, the National Police Chiefs' Council (UK) approved the Agreement on the use of artificial intelligence (AI) in policing²¹. This

document is interesting enough to be studied since it outlines the definition and



¹⁹ The Artificial Intelligence and Data Act (AIDA) – Companion document. URL: <https://isde-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s10>

²⁰ Christopher Ferguson, Heather Whiteside Bill C-27: Federal Government Releases Amendments to Canada's Proposed AI Law // Privacy & Cybersecurity Bulletin. DECEMBER 7, 2023. URL: <https://www.fasken.com/en/knowledge/2023/12/bill-c27-federal-government-releases-amendments-to-canadas-proposed-ai-law#authors>

²¹ Covenant for Using Artificial Intelligence (AI) in Policing. National Police Chiefs' Council. URL: https://science.police.uk/site/assets/files/4682/ai_principles_1_1_1.pdf

characteristics of AI, principles of its application, distribution of responsibility and authority among police officers.

The use of the Prometea Artificial Intelligence System in the work of courts and law enforcement officers in Argentina during the proceedings on administrative violations and the decisions thereon has demonstrated notable results. In particular, the Prometea AI system is capable of issuing and formalizing a court decision in a number of categories of administrative cases within 10 seconds. Therefore, we can confidently talk about the efficiency and cost-effectiveness of procedural decision-making with the use of AI ²².

Conclusions. Summarizing the above, we can emphasize that the analysis of documents and legislative experience in the EU, the US and other developed countries enables us to identify common trends and principles in the use of AI technologies within law enforcement:

All analyzed legal regulations are aimed at protecting and preserving the fundamental rights of a human being, guaranteeing his/her health and safety during AI application, as well as ensuring the overall democratic functioning of society.

The principles of accountability, transparency and fairness are present in almost all AI governance structures. Now they have acquired the status of common standards, as evidenced by their consistent presence in the regulatory acts on AI regulation.

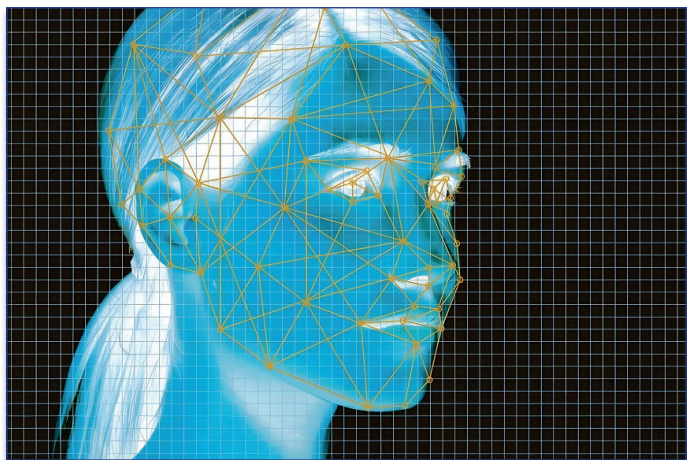
Distinguishing between different forms of AI: each of these regulations distinguishes between different kinds of AI systems, either by reference to the impacts they generate, the risks they pose, the context in which they're used, or the specific kind of system they are. At a higher level, each regulation also exhibits an increased concern for the development and deployment of high-risk or high-impact AI systems, though none possess a tiered risk classification structure as sophisticated as that of the EU AI Act ²³.

However, despite the existing achievements, the issue of implementing AI in the work of law enforcement and police officers remains controversial and is accompanied by various approaches: from active use of AI during the resolution of administrative cases of different categories to establishing criminal liability for the use of AI algorithms to forecast court decisions during the hearing of administrative cases ²⁴. After all, AI enables to boost the data processing process, reduce the workload of law enforcement officers and judges, and make it more efficient. At the same time, we should not forget about the observance of fundamental principles when using AI: the rule of law, lawfulness, non-discrimination, impartiality, fairness, information security, etc. Given the above, we believe that Ukraine also needs to adopt

²² Казанчук, І. Д. Правові засади використання штучного інтелекту в діяльності правоохоронних органів (поліції) та органів суду під час здійснення адміністративного провадження (аналіз зарубіжного та українського досвіду) // Право.ua. - 2023. - № 4. - С. 63-69. URL: <https://dspace.univd.edu.ua/items/e911b080-60a7-442f-87ab-67a1bf2d7b0e>

²³ Analysis: Canada's Artificial Intelligence and Data Act. MAY 10, 2024. URL: <https://www.lumenova.ai/blog/canada-artificial-intelligence-and-data-act-analysis/>

²⁴ Казанчук Ірина. Можливості використання штучного інтелекту в діяльності судової гілки влади: проблеми та перспективи правового регулювання // Актуальні проблеми адміністративно-деліктного права України : матеріали круглого столу (м. Вінниця, 31 жовт. 2023 р.). Вінниця : ХНУВС, 2023. С. 35-38. URL: <https://dspace.univd.edu.ua/items/b05bd590-e681-4445-9381-7a9e003303e8>



corresponding legislation and by-laws that would govern social relations that develop when using AI capabilities in law enforcement.

Reference

- Blueprint for an AI Bill of Rights. The White House. URL: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>
- Christopher Ferguson, Heather Whiteside Bill C-27: Federal Government Releases Amendments to Canada's Proposed AI Law //Privacy & Cybersecurity Bulletin. December 7, 2023. URL: <https://www.fasken.com/en/knowledge/2023/12/bill-c27-federal-government-releases-amendments-to-canadas-proposed-ai-law#authors>.
- Covenant for Using Artificial Intelligence (AI) in Policing. National Police Chiefs' Council. URL: https://science.police.uk/site/assets/files/4682/ai_principles_1_1_1.pdf
- ENISA, About ENISA. URL: <https://www.enisa.europa.eu/about-enisa>
- European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. European commission for the efficiency of justice (CEPEJ). Strasbourg, 3-4 December 2018. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>
- European Union Agency for Network and Information Security (ENISA), 'ENISA: 15 years of building cybersecurity bridges together', Press release, 20 March 2019. URL: <https://www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together>
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The White House, October 30, 2023. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/?utm_source=link
- Razmetaeva, Yu, Barabash, Yu, Lukianov, D (2022). 'The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice' 2022 3(15) Access to Justice in Eastern Europe. 41-56. URL: https://ajee-journal.com/upload/attaches/att_1660480856.pdf
- Tancrede Montagne Overview of the AI Act, the first ever legal framework on AI. 26. March 2024. URL: <https://paytechlaw.com/en/overview-of-the-ai-act-the-first-ever-legal-framework-on-ai/>
- The Artificial Intelligence and Data Act (AIDA) Companion document. URL: <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s10>
- Hutsu, S.F. (2021). Uprovazhennia shchuchnoho intelektu v trudovi vidnosyny: perspektyvy pravovoho rehuliuвання. *Visnyk NTUU «KPI»*. Politolohiia. Sotsiolohiia. Pravo. Vypusk 2 (50) 87-92. URL: <http://socio-journal.kpi.kiev.ua/archive/2021/2/16.pdf> [in Ukrainian].
- Kazanchuk, I. D. (2023). Pravovi zasady vykorystannia shchuchnoho intelektu v diialnosti pravookhoronnykh orhaniv (politsii) ta orhaniv sudu pid chas zdiisnennia administratyvnoho provadzhennia (analiz zarubizhnogo ta ukrainskoho dosvidu). *Pravo.ua*. № 4. 63-69. URL: <https://dspace.univd.edu.ua/items/e911b080-60a7-442f-87ab-67a1bf2d7b0e> [in Ukrainian].
- Katerynychuk, I. (2015). Mizhnarodnyi ta zarubizhnyi dosvid zastosuvannia informatsiinykh tekhnolohii u diialnosti pravookhoronnykh orhaniv. *Natsionalnyi yurydychnyi zhurnal: teoriia ta praktyka*. Cherven. 22-26. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/efd04dce-59c5-49cd-b868-a14881450289/content> [in Ukrainian].
- Koznova, O. Yevroparlament ukhvalyv Zakon pro shchuchnyi intelekt URL: https://biz.ligazakon.net/news/226272_vroparlament-ukhvaliv-zakon-pro-shtuchniy-ntelekt [in Ukrainian].

- Kontseptsiiia rozvytku shtuchnoho intelektu v Ukraini. Skhvaleno rozporiadzhenniam Kabinetu Ministriv Ukrainy vid 2 hrudnia 2020 r. № 1556-p. URL: <http://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> [in Ukrainian].
- Krasnikov, D. Novyi ukaz Prezidenta Baidena pro shtuchnyi intelekt: bilshе obmezhen chy stymuliuvannia rozvytku. 15.11.2023. URL: <https://www.ukrinform.ua/rubric-technology/3787099-novij-ukaz-prezidenta-baidena-pro-stuchnij-intelekt-bilse-obmezen-ci-stimuluvanna-rozvitku.html> [in Ukrainian].
- Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 01.12.2022 №2807-IX Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> [in Ukrainian].
- Propozytsiia shchodo Rehlamentu Yevropeiskoho Parlamentu ta Rady, shcho vstanovliuie harmonizovani pravyla shchodo shtuchnoho intelektu - Vidpovidnist pravovykh osnov statei 114 i 16 DFleS shchodo polozhen, shcho zastosovuiutsia do pravookhoronnykh i sudovykh orhaniv (dokument Rady 12302/22) , LIMITE, 12 veresnia 2022 r., pdf). Brussels, 12 September 2022. URL: <https://www.statewatch.org/media/3510/eu-council-ai-act-law-enforcement-legal-basis-cls-12302-22.pdf> [in Ukrainian].
- Reutov, I. Pravove rehuliuвання shtuchnoho intelektu: mizhnarodnyi dosvid ta ukraïnski perspektyvy. URL: <https://pravo.ua/pravove-rehuliuвання-shtuchnoho-intelektu-mizhnarodnyi-dosvid-ta-ukraïnski-perspektyvy/> [in Ukrainian].
- Stymuliuvannia innovatsii ta vprovadzhennia shtuchnoho intelektu v Yevropi. URL: <https://finap.com.ua/stymulyuvannya-innovatsij-ta-vprovadzhennya-shtuchnogo-intelektu-v-yevropi/> [in Ukrainian].
- Uhoda mizh Ukrainoiu ta Yevropeiskym politseiskym ofisom pro operativne ta stratehichne spivrobitnytstvo, ratyfikovana Zakonom vid 12.07.2017 № 2129-VIII.// Ofitsiinyi visnyk Ukrainy. Vid 08.08.2017, 2017 r., № 62, / № 71, 2017, st. 2192. URL: https://zakon.rada.gov.ua/laws/show/984_001-16#Text [in Ukrainian].
- Uhoda mizh Ukrainoiu ta Yevropeiskym politseiskym ofisom pro stratehichne spivrobitnytstvo : Zakon Ukrainy vid 5 zhovtnia 2010 roku № 2576-VI // Ofitsiinyi visnyk Ukrainy. 2010. № 96/№ 84. St.2934/3432. URL: https://zakon.rada.gov.ua/laws/show/994_954#Text [in Ukrainian].

Received by Editorial Board: 5.04.2024

Suggested Citation:

Kaliuzhnyi, D. (2024). Legal Grounds For Artificial Intelligence Use In Law Enforcement: International And Foreign Experience. *Archives of Criminology and Forensic Sciences*. 1 (9). 103-113. DOI: <https://doi.org/10.32353/acfs.9.2024.08>

