KONRAD ADENAUER STIFTUNG

International Approaches to AI Development and Principles of Responsibility for Use: Conclusions for Ukraine

Olha Petriv, Olena Spesyvtseva

www.kas.de

Publisher
Konrad-Adenauer-Stiftung Ukraine (Kyiv)

Authors
Olha Petriv, Lawyer on artificial intelligence at Independent Media Direction of the Centre for Democracy and Rule of Law;
Olena Spesyvtseva, Lawyer on copyright and media law at Independent Media Direction of the Centre for Democracy and Rule of Law.

The publication is prepared under the project "Strengthening the Analytical Capabilities of the Foreign Policy Decision-Making with the Civil Society" of the Centre for International Security with the support of the Konrad-Adenauer-Stiftung Ukraine (Kyiv).

wul. Akademika Bohomoltsia 5, Office 1, 01024 Kyiv, Ukraine
Telephone: +380444927443
https://www.kas.de/en/web/ukraine

Borodina Inzhenera Street, 5-A, 02092 Kyiv, Ukraine
Telephone: +380999833140
https://intsecurity.org/

M. Zankovetskoi Street, 3/1, office 12, Kyiv, 01001
Telephone: +380678282074
info@cedem.org.ua
https://cedem.org.ua
https://www.facebook.com/CEDEMUA/

Table of contents

Introduction

The rapid development of artificial intelligence (hereinafter – AI) has formed a contradictory attitude towards it. AI is recognized as a powerful tool for economic growth of states, development of innovation and increasing productivity and efficiency of work in various spheres – from healthcare and culture to national security and justice. On the other hand, it is obvious that the application of AI tools is accompanied by risks related to discrimination, interference with privacy, threats to personal data, and lack of transparency in decisions. This dual perception requires balanced approaches to AI regulation that will implement effective control mechanisms and legal responsibility while promoting, rather than limiting, technological development.

AI development from its very beginning was driven by national security needs. And if today Ukraine's state policy in the spheres of national security and defense is comprehensively directed at ensuring military, foreign policy, state, economic, information, environmental security, critical infrastructure security, cybersecurity of Ukraine and other directions, then the development of artificial intelligence systems can undoubtedly contribute to the fulfillment of this task.

Today, fundamentally important questions arise concerning ethical, legal and strategic aspects of AI use:

- How to ensure reliability and safety of AI systems functioning in conditions of military conflict?
- How to guarantee respect for human rights when implementing AI in the security sphere?
- Who will bear responsibility for AI decisions?
- How to prevent discriminatory practices and bias in algorithms?
- How to achieve transparency and accountability of AI systems, particularly when using them for processing large volumes of personal data?
- How to maintain the balance between innovation and regulation so as not to slow down development but also not allow abuse?

These questions require not only professional analysis, but also the formation of a comprehensive national policy on AI use in the security context that would correspond to international standards, national interests and rule of law principles.

Therefore, today on the agenda of leading states and regions of the world is the formation of an approach to AI regulation that combines ethical principles, legal and

security guarantees. For example, the European Union's (hereinafter – EU) approach is preventive and oriented towards human rights and national security. The United States prefers flexibility, stimulating AI development through partnership with the private sector and gradual formation of recommendations. However, the experience of both regions is important for Ukraine, where the EU model serves as a reference point for legal harmonization, while borrowing US experience can contribute to innovation development.

It is worth mentioning that back in December 2020, the Cabinet of Ministers of Ukraine approved the Concept of Artificial Intelligence Development in Ukraine, which defines the purpose, principles and tasks of AI technology development in Ukraine as one of the priority directions in the field of scientific and technological research. It mentions problems that need to be solved, including, in particular, the low level of digital literacy of the population regarding general aspects, opportunities, risks and safety of AI use, absence or imperfection of legal regulation of AI, low level of investment in AI technology development, absence of unified approaches applied in determining ethics criteria during development and use of AI technologies for different industries, types of activities and spheres of the national economy, etc.

Solving these problems undoubtedly requires a comprehensive approach: analysis of AI regulation practices in other states and regions, development of legislative initiatives and comprehensive principles for using AI systems, consultations with stakeholders (including both developers and users of AI systems, as well as investors and government representatives).

The Concept of Artificial Intelligence Development in Ukraine has already defined principles for AI technology development and use, which, although advisory, can serve as a guideline. Among the principles are in particular:

- Development and use of AI systems only under conditions of adherence to the rule of law, fundamental human and citizen rights and freedoms, democratic values, as well as ensuring appropriate guarantees when using such technologies;
- Compliance of activities and decision-making algorithms of AI systems with requirements of personal data protection legislation, as well as observance of the constitutional right of everyone to non-interference in personal and family life in connection with personal data processing;
- Ensuring transparency and responsible disclosure of information about AI systems, reliable and safe functioning of AI systems throughout their entire life cycle and ongoing assessment and management of potential risks;
- Placing responsibility on organizations and persons who develop, implement or use AI systems for their proper functioning in accordance with the specified principles, etc.

EU Approach to AI Development and Principles of Responsibility for Use

Results of multi-year discussions of opportunities, challenges and risks associated with AI systems development are gradually finding consolidation in regional and national legal sources. There is a transition from declarations, recommendations on responsible use of AI systems or internal rules (codes) of conduct of individual organizations to the adoption of normative legal acts.

A response to the need for regulating AI technologies and their impact on society due to rapid AI development in the EU has become, in particular, the Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, hereinafter – AI Act) – an EU regulation that entered into force on August 1, 2024, whose purpose is to create a safe environment for AI use and development.

For Ukraine, studying EU experience is of fundamental importance for several reasons. In a situation where AI technologies are already actively used, but specialized legislation has not yet been formed, there is an urgent need to implement clear standards for AI development and use. When forming its own regulatory model, Ukraine should take into account the EU approach, which corresponds to the strategic course towards European integration and obligations arising from the Association Agreement with the EU. In addition, the EU today acts as a global leader in the field of digital regulation, an example of which is the adoption in 2016 of the General Data Protection Regulation (GDPR), which is aimed at protecting natural persons with regard to the processing of their personal data and the free movement of such data.

The AI Act does not apply to all AI systems. Systems that are placed on the market, put into service or used for military, defense or national security purposes are excluded from its scope regardless of what type of entity carries out such activity (public or private entity). National security remains the exclusive responsibility of Member States in accordance with Article 4(2) of the Treaty on European Union.

However, if such an AI system (developed and used for military, defense or national security purposes) is simultaneously used outside these purposes (for example, for civilian or humanitarian purposes, law enforcement or public safety purposes), such a system falls under the AI Act. In such a case, the entity using the AI system for purposes other than military, defense or national security must ensure AI systems compliance with AI Act requirements.

The AI Act consists of 12 chapters, each regulating a separate sphere of AI application and development. The main provisions of this legislative act provide for (more details via link):

1. Definition of AI systems risk levels (prohibited AI systems, high-risk AI systems, limited risk AI systems, minimal risk or non-risk AI systems).

2. Introduction of mandatory certification for certain AI systems (biometric identification systems, critical infrastructure, educational or professional assessment systems).

3. Establishment of requirements for certain AI systems regarding the need to inform users that they are interacting with an AI system, not a human.

4. Establishment of transparency rules for AI systems designed to interact with natural persons, emotion recognition systems, as well as AI systems used to create or manipulate image, audio or video content.

5. Creation of a single European AI market – introduction of unified rules for working with AI technologies in EU territory, which will promote free movement of AI systems and services in the European market.

6. Prohibition of using certain AI methods. For example, it is prohibited to place on the market and use AI systems that apply techniques going beyond human consciousness, forcing certain decisions.

Regarding responsibility, the AI Act emphasizes that it is appropriate for a specific natural or legal person, defined as a provider of AI systems, to bear responsibility for placing on the market or putting into service a high-risk AI system, regardless of whether this natural or legal person is the one who designed or developed the system.

At the same time, the scientific community criticizes that responsibility in the AI Act does not have an imperative character, and the prohibition of discrimination is only implicit. This indicates the further need to improve legislation taking into account new challenges.

The foundation of this AI systems regulation model is the combination of legal and ethical principles: transparency, fairness, respect for human rights, avoidance of discrimination, human control and harm prevention. The EU has laid the foundations for a regulation system that in the context of national security is based on prohibiting systems with unacceptable risk levels, enhanced regulation of high-risk systems, obligating AI system providers to comply with data management, transparency and cybersecurity procedures, placing responsibility for AI systems compliance on developers and providers.

Implementation of AI Act Provisions in Legislation of Ukraine

The AI Act today is an instrument that introduces a comprehensive approach to regulating the development and safe application of AI tools in various spheres of human and state activity. But each separate sphere requires implementation and adaptation to its specifics.

For example, today in Ukraine regulation of AI work results use occurs according to the Law of Ukraine "On Copyright and Related Rights". The AI Act emphasizes that general purpose AI models capable of generating text, images and other content open unique opportunities for innovation, but also pose challenges for artists, authors and other creators, as well as for the way their creative content is created, distributed, used and consumed. Development and training of such models require access to vast amounts of text, images, video and other data. Any use of copyright-protected content requires permission from the respective rights holder, unless appropriate copyright exceptions and limitations apply.

AI regulation can also, moreover must, occur according to the Law of Ukraine "On Personal Data Protection". For example, the AI Act defines that any processing of personal data related to using AI systems for biometric identification is prohibited, except in cases related to using biometric identification systems for law enforcement purposes. Since AI can perform automatic processes of collecting and processing personal data, for example, for analyzing user behavior on websites or for developing personalized advertising campaigns, the Law of Ukraine "On Personal Data Protection" must contain requirements for personal data processing during AI systems functioning. In particular, this concerns their collection, storage, use, transfer and protection, requirements for automated data processing, prohibition of biometric identification without special permission, security guarantees when using AI in public administration.

Currently Ukraine participates in AI Act implementation through introducing regulatory "sandboxes", whose creation is discussed in Chapter 5 of the AI Act. Regulatory "sandboxes" are a safe and controlled space for experiments that national competent authorities must create at the national level to facilitate development and testing of innovative AI systems under strict regulatory supervision before these systems are released to the market or put into service.

In particular, the possibility of processing personal data for developing certain AI systems in the public interest in regulatory "sandboxes" is separately regulated by the AI Act. Thus, they can be processed for the purpose of developing, training and testing certain AI systems in a sandbox if the following conditions are met, including:

1. AI systems are developed for protecting substantial public interests by a public body or other natural or legal person;

2. There are effective monitoring mechanisms to detect any high risks to the rights and freedoms of data subjects that may arise during the experiment;

3. Personal data subject to processing in the sandbox context are in a functionally separate data processing environment under the provider's control, and only authorized persons have access to this data;

4. Personal data cannot be transferred outside the sandbox, are protected by appropriate technical and organizational measures and deleted after participation ends;

5. A brief summary of the AI project developed in the sandbox, its objectives and expected results is published on the competent authorities' website and other conditions.

The AI Act defines that EU Member States must ensure that their competent authorities create at least one regulatory "sandbox" for artificial intelligence at the national level, which must be operational by August 2, 2026. Given Ukraine's rapid European integration movement, national competent authorities should consider that, although the specified deadline does not apply to Ukraine, the AI Act will automatically extend to Ukraine immediately after gaining membership, and therefore work on creating regulatory sandboxes continues and has first results.

The Ministry of Digital Transformation and Ukrainian Startup Fund announced the launch of Sandbox – a "sandbox" for Ukrainian companies offering high-tech solutions for digital economy spheres, general infrastructure, public services, optimization of public authorities' work, healthcare, biotechnology, education and science, agricultural sector, defense, etc.

The trend towards further implementation of regulatory "sandboxes" demonstrates the need to establish clear national legislation requirements for personal data protection, ethical verification, control over training and testing systems in such "sandboxes". In December 2020, the Cabinet of Ministers of Ukraine approved the Concept of Artificial Intelligence Development in Ukraine, in October 2023 the Roadmap for Artificial Intelligence Regulation in Ukraine was presented, and in June 2024 the White Paper on AI Regulation in Ukraine was presented. The White Paper on AI regulation devotes special attention to self-regulation as a tool for forming ethical standards and complementing state policy. In June 2025, 14 leading Ukrainian companies signed the Memorandum on Self-Regulation in the Field of AI, taking on voluntary commitments regarding safe and transparent technology development.

Recommendation documents and national strategy formation serve as guidelines in the field of AI and are an integral component of forming a culture of development, market introduction and use of AI systems. However, the state's primary task today is developing a regulatory framework in various spheres, particularly regarding responsibility for decisions made or executed by AI systems, with differentiation of developer, user, provider and state obligations.

Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and Rule of Law as Guideline for Ukraine

Ukraine must develop a regulatory framework for AI regulation, as in 2025 it joined the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and Rule of Law (hereinafter – AI Convention). This is the first binding treaty in the field of AI that covers the entire life cycle of AI systems. Each state takes measures to ensure accountability and responsibility for negative impact on human rights, democracy and rule of law arising from activities throughout the life cycle of artificial intelligence systems.

The explanatory note to the AI Convention states that the principle of accountability and responsibility concerns the need to create mechanisms through which persons, organizations or entities responsible for activities within the AI systems life cycle will bear responsibility for negative impact on human rights, democracy or rule of law. States are required to create mechanisms that can be applied to activities throughout the AI systems life cycle to ensure fulfillment of this requirement. This may include judicial and administrative measures, civil, criminal and other liability regimes, and in the public sector – administrative and other procedures so that decisions can be challenged.

It is necessary to clearly distribute responsibility and possibilities to track actions and decisions of specific persons or entities taking into account the diversity of relevant participants and their roles and obligations. All entities responsible for activities within the AI systems life cycle, regardless of whether they are public or private organizations, must be subject to the existing system of rules, legal norms and other relevant state mechanisms.

Ukraine's approach for identifying, analyzing, assessing risks and impact of AI systems on human rights, democracy and rule of law today can develop based on HUDERIA (Human Rights, Democracy, and the Rule of Law Impact Assessment) methodology developed by the Committee on Artificial Intelligence (CAI) of the Council of Europe (more details via link), which consists of several stages: AI system risk identification, impact assessment, management assessment (responses to socio-technical issues and issues concerning human rights, democracy and rule of law), negative impact mitigation and AI system assessment. The methodology can be used by both state institutions and private entities. It does not have binding legal force, while states – parties to the AI Convention – can flexibly use or adapt it fully or partially to their own national interests. The methodology can contribute to ensuring that AI sphere developments do not violate human rights, comply with democratic principles and rule of law.

US Approach to Artificial Intelligence Regulation

American artificial intelligence regulation policy from the beginning is built on internal tension: Washington seeks to maintain technological leadership, but simultaneously faces increasingly loud demands regarding safety, human rights and competitive balance. From Biden's October Executive Order – EO 14110 (2023) – to the "deregulatory" EO 14179 (January 2025), the White House has traveled a path from attempting to establish mandatory "safeguards" to signaling liberalization for business. Such rapid course change created a "pendulum policy" situation: the market receives contradictory impulses, while the legislature still has not managed to give a comprehensive response (Federal Register, The White House).

Executive Order EO 14110 introduced eight general principles for AI development and implementation: safety and security, protection of consumer rights, privacy and civil liberties, fairness, transparency and explainability, risk management, innovation and competition, US global leadership.

The National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) were tasked with developing risk assessment standards. The Order also first obligated federal agencies to publish AI Impact Assessments for critical systems. In practice, the document remained primarily "soft law", having a recommendatory character – it provided no sanctions for non-compliance.

However, already in January 2025, another executive order – EO 14179 – cancelled a number of previous restrictions. It was signed by President Donald Trump, arguing this with the desire to preserve US global technological leadership.

To avoid leaving AI uncontrolled, two months later the US Office of Management and Budget issued memorandum M-24-10. It addressed minimum requirements for the most powerful AI models, which include safety testing, external audits and maintaining algorithm operation logs.

Legislative "Mosaic": Congress, State Experiments and Institutional Division

In the 119th Congress, several important bills are under consideration simultaneously. All these initiatives demonstrate the following trend: Congress solves complex AI issues with "targeted" laws (congress.gov, congress.gov, WIRED).

An example of the targeted approach is the TAKE IT DOWN Act, submitted to the Senate in January 2023. The bill criminalizes creation and distribution of sexualized deepfake images without victims' consent. Its territorial scope covers all US states. This is the first case when Congress specifically addresses a concrete technology, not all AI in general.

Under consideration in Congress is the CREATE AI Act (H.R. 2385), introduced in March 2023. It provides for creating public computing clusters for scientists to ensure equal access to computational capacities that are now concentrated in private cloud giants. The law contains no model safety requirements.

Another important project is the American Privacy Rights Act (APRA), introduced in March 2024. It aims to unify the approach to personal data protection at the federal level, but is currently stuck at the discussion stage in the House Energy Committee.

All these initiatives demonstrate: instead of creating a unified AI law, the US implements targeted interventions through separate sectoral or thematic acts. Comparing US and EU approaches, we can say that the EU chose a broad approach and introduces general AI regulation principles, while the US has a sectoral approach. Ukraine should find a golden mean.

AI regulation experiments are conducted at the state level. In Texas, SB 1621 signed in June 2023 criminalizes creating deepfake images involving minors. The law operates only within the state. SB 20, passed in May 2025, signed June 20, 2025, prohibits possession, distribution and creation of AI-generated child pornography. It provides for up to 2 years imprisonment and fines up to $10,000. In Virginia, HB 697 (2024) introduces criminal liability for using "synthetic media" for fraud purposes. The law provides a new category of crimes. In Tennessee, the ELVIS Act protects artists from unauthorized use of voice or image using AI. The law entered into force July 1, 2024. In Utah, SB 149 – Utah SB 149 (Artificial Intelligence Policy Act) entered into force May 1, 2024 and provides for creating an AI Policy Office, launching the "AI Learning Lab" pilot program for testing generative AI systems, and establishing requirements for disclosing AI use during user interaction. Initially it operated only until May 1, 2025, but was extended until July 1, 2027 through amendments (SB 226 and SB 332). The law remains in effect and requires transparency and caution from all who use generative AI in Utah. Local Law 144 in New York entered into force July 5, 2023 and prohibits automated hiring tools without prior bias audits.

The US has no unified artificial intelligence regulator – instead a network coordination model operates. Individual agencies are responsible for different directions:

1. NIST (National Institute of Standards and Technology) – developed AI Risk Management Framework 1.0 (AI RMF), and in July 2024 presented a specialized profile for generative AI. This document describes 12 specific generative AI risks (for example, false facts, data leaks, environmental burden) and proposes over 200 specific actions for their management. Although the profile is voluntary, it has actually become a standard that companies follow.

2. OSTP (Office of Science and Technology Policy at the White House) – sets the direction of political discussion. In 2022 it presented the Blueprint for an AI Bill of Rights, and after presidential executive order EO 14179 coordinates the interagency AI Action Plan.

3. NSF (National Science Foundation) – administers the NAIRR (National AI Research Resource) pilot program. Its goal is to provide scientists access to computational resources and open datasets to level the playing field with Big Tech (logic – "democratize computing").

4. DARPA (Defense Advanced Research Projects Agency) – works on interpretable AI systems (XAI 2.0) and safety tools (Guardrails). The agency often uses classified data, which complicates independent assessment.

5. DoD / CDAO (Department of Defense / Chief Digital and AI Office) – after the Task Force Lima initiative (2023-2024) created the AI Rapid Capabilities Cell with a $100 million budget (for 2024-2025). The cell works on 15 combat use scenarios for generative AI.

Thus, in the US, AI regulation functions are distributed among many institutions, and although there is no centralized oversight, the institutions form a powerful system of coordinated risk management, similar to the cybersecurity model.

AI Use in US National Security

In the US national security sphere, a separate and significantly less public artificial intelligence management regime is applied. The Department of Defense (DoD) develops its own protocols and policies that significantly differ from civilian regulation. Formally, the human-in-the-loop principle is maintained, meaning human participation in decision-making processes. At the same time, this principle is applied flexibly: human control is implemented only where it does not contradict operational or combat requirements. Within clearly defined and technically controlled scenarios, artificial intelligence systems can operate with partial or full autonomy.

Generative AI use in the defense sector is integrated into digital combat infrastructure through JWCC (Joint Warfighting Cloud Capability) – a cloud platform that combines Amazon, Microsoft, Google and Oracle services. It provides continuous access to data, computational resources and analytical tools in real time to support missions. Although JWCC does not perform direct AI monitoring functions, it is the main environment for their deployment. The level of transparency in this sphere is significantly lower than in civilian use: most model characteristics, testing methodologies and audit results are not disclosed, which limits independent technology assessment.

In August 2023, the Department of Defense initiated Task Force Lima – an interagency working group to study generative AI potential in the defense context. In December 2024, its activity was institutionalized in the form of a permanent unit – AI Rapid Capabilities Cell (AI RCC) – with a $100 million budget for 2024-2025. AI RCC deals with implementing generative AI in a number of priority directions, such as intelligence analysis, operation planning, information influence, logistics and supporting command and control processes.

US Structural Challenges

The US still lacks a comprehensive federal law similar to the European AI Act. Instead, a fragmented ecosystem is forming – Congress acts selectively, while states pass their own regulations, leading to a "compliance puzzle" with 50 different regimes. Companies are forced to navigate simultaneously local, federal and even international law, lacking a clear strategic framework.

The regulatory trajectory also remains inconsistent. On one hand, presidential executive order EO 14179 stimulates innovation development by simplifying access to computational resources and data. On the other hand, memorandum OMB M-24-10 establishes strict requirements for federal agencies regarding AI systems testing, auditing and transparency. This creates a "regulatory pendulum" effect where the market lacks a clear answer: deregulation or control.

At the ethical level, the issue of deepfake manipulations arises acutely. In response to growing such risks, states independently implement regulation: Texas (SB 20) criminalizes creating AI-generated child pornography, while Virginia (HB 697) prohibits distributing altered images with sexual subtext without the depicted person's consent.

At the intersection of ethics and security is the issue of transparency in national security. Most Department of Defense initiatives, particularly within Task Force Lima or AI RCC, are conducted behind closed doors. On one hand, this ensures operational advantage and rapid technology implementation. On the other hand, lack of independent audit undermines trust in decisions that can potentially affect security, human rights and international stability.

The US demonstrates a paradox: the world's largest AI driver still remains without a "unified" AI law. Instead, they rely on soft-law (NIST RMF), narrow criminal and private initiatives (TAKE IT DOWN, state deepfake acts) and rapid defense initiatives.

Conclusions and Recommendations for Ukraine

Ukraine has a chance to adapt international AI approaches to its own needs, especially in the national security sphere, which includes cyber defense, combating information threats, critical infrastructure protection and border control.

Ukraine's further steps in the context of AI systems development and implementation should concern the following:

1. Formation of a national strategy that will become a guideline in the AI sphere and an integral component of forming a culture of development, market introduction and use of AI systems.

2. Formation of a comprehensive regulatory framework for AI regulation. An important step towards implementing AI systems regulation and their effective functioning is information and educational activities among citizens and Ukrainian business, which will help form a sustainable understanding of how to increase productivity, effectiveness, production using AI, how to protect oneself from risks and negative consequences of AI use.

3. Harmonization with the AI Act particularly regarding AI systems classification by risk level, transparency requirements, user information, safety, establishing the principle of responsibility for AI systems providers and developers. Today Ukraine should choose the path of voluntary and initiative approximation to EU law, which is currently not mandatory for implementation.

4. Adopt recommendations concerning artificial intelligence risk management systems (analog of RMF based on NIST; the NIST AI RMF 1.0 framework offers practical guidelines for AI risk management). This is important for a unified approach to risk assessment in national security (for example, when assessing developments for the Ministry of Internal Affairs, Security Service of Ukraine or State Border Guard Service), allows using it as a requirement in state AI systems procurement, reduces bureaucratic burden. Implementation should include, in particular, the following steps: RMF translation, adaptation as voluntary DSTU (State standards of Ukraine) recommendation, recommendation for application in the public sector, primarily in national security bodies.

5. Guarantee of human control in critical AI decisions and ensuring public control, involving the expert community in risk assessment when implementing new AI systems. Within national security, AI should be applied with guaranteed human control, especially in spheres of automated threat detection, border person verification, cyber risk analysis. Normatively establish the principle "human makes

the final decision", prohibit full autonomy in critical scenarios, implement simulation testing and logging of AI decisions in security systems.

6. Creation of a special independent AI ethics body or unit within existing ones that will control compliance with human rights in AI application. In particular, create a Coordination Council on AI under the Cabinet of Ministers of Ukraine with a security mandate. The American OSTP approach demonstrates the advantage of network governance without excessive centralization. Thus, the Coordination Council on AI under the Cabinet of Ministers should include representatives of the Ministry of Digital Transformation, Ministry of Internal Affairs, Security Service of Ukraine, National Academy of Sciences of Ukraine, National Coordination Center for Cybersecurity, Defence Intelligence of Ukraine and adopt methodological recommendations for implementing safe AI in public structures.

7. Promoting investment attraction in the AI sphere through public-private partnerships, startup and research institution support.

8. Integration into international AI standards development initiatives, particularly within the Council of Europe and EU.

9. Launch of pilot project "U-AIRR" (Ukrainian Artificial Intelligence Research Resource) – national AI resource for security and science. Analog of NAIRR in the US – this is public access to GPU resources for scientists and security institutions. In Ukraine, the project can be implemented based on specialized state cloud infrastructure in partnership with private providers under Ministry of Digital Transformation coordination. Access to GPU resources can be provided within grant support for teams working on AI in security, defense, disinformation combating and threat detection spheres.

10. Deepfake regulation in political advertising. US states, particularly Texas and Virginia, have already passed laws limiting AI use for public opinion manipulation. In Ukraine, it is recommended to amend the Electoral Code to require disclosure of AI or deepfake use in political campaigning.

For Ukraine, a combined approach is valuable: voluntary standards, targeted legislation and interagency coordination, which allows not blocking innovation but also not leaving gaps in critical sectors.