ARTIFICIAL INTELLIGENCE TECHNOLOGY IN UKRAINE'S ELECTORAL SYSTEM: IMPLEMENTATION PROSPECTS

Kurashov Oleksii

DOI: https://doi.org/10.61345/1339-7915.2024.3.18

Annotation. The article is dedicated to examining the issues related to the implementation of artificial intelligence technologies in Ukraine's electoral system. Based on an analysis of ChatGPT technology, the author explores the potential threats and risks to the national electoral system arising from the adoption of such technologies. Additionally, the article reviews foreign legislation regulating the implementation and functioning of artificial intelligence technologies in the electoral systems of European Union countries.

Key words: electoral system, artificial intelligence, ChatGPT, e-governance.

1. Introduction.

Artificial Intelligence (AI) has become a powerful tool thanks to technological progress, access to large amounts of data, machine learning, and increased computational power. The emergence of ChatGPT at the end of 2022 marked a new breakthrough in the use of AI. The wide range of capabilities of Artificial General Intelligence (AGI) to solve a broad spectrum of tasks and the development of generative AI to create synthetic content based on user requests have become evident. In just a few years, a significant portion of online content may be created synthetically. In the context of studying the constitutional and legal regulation of the use of innovative technologies in the electoral process in Ukraine, it is impossible to ignore the vast range of possibilities that AI can offer within Ukraine's electoral system.

2. The aim of the work is to explore the legal challenges of implementing artificial intelligence within Ukraine's electoral system as one of the most advanced innovative technologies in the world. The focus is on the following issues: the legal status of artificial intelligence, its impact (negative or positive) on democratic processes in the state in case of the introduction of AI elements, the risks of implementing artificial intelligence, and international experience.

3. Analysis of scientific publications.

The issues of implementing artificial intelligence in various spheres of public life in Ukraine and abroad have long been the subject of research by legal scholars. For instance, S. Asiryan, in his works, focuses on analyzing the measures that European Union countries are taking to ensure the protection of citizens' constitutional rights in the context of the implementation of artificial intelligence in various spheres of public life [1]. In turn, T. Katkova studies the general aspects of implementing artificial intelligence in the legal sphere of our state, as well as the prospects for legislative regulation of the implementation of artificial intelligence in the context of the introduction of robotic technology [2].

O. Kurakin and O. Skryabin, in their joint work, examine the peculiarities of legal regulation of the use of artificial intelligence in Ukraine and identify opportunities for enhancing its effectiveness [3].

A. Frantsuz, N. Stepanenko, and A. Shevchenko address the issue of artificial intelligence through the lens of protecting human rights and freedoms during the electoral process [4].

In our opinion, the rapid implementation of advanced innovative technologies in all spheres of public life today is axiomatic, and the electoral process should not be an exception. However, we should not limit ourselves to the issue of electronic voting, as it is only one of the elements or types of AI application. It is necessary to explore the vast array of innovative technologies that are components of AI. It becomes evident that studying the peculiarities of implementing AI systems in the field of constitutional and electoral law requires extraordinary attention. Any technologies introduced into the electoral process must guarantee the protection of electoral rights and freedoms. It is essential to clearly identify the positive and negative consequences of such implementation within the study of ways to improve the electoral process in Ukraine.

4. Review and discussion.

The definition of AI is provided in the Concept for the Development of Artificial Intelligence in Ukraine dated December 2, 2020, No. 1556-r. According to this document, artificial intelligence is an organized set of information technologies that can perform complex tasks by using a system of scientific research methods and algorithms for processing information obtained or independently created during operation. It also includes the ability to create and use its own knowledge bases, decision-making models, information processing algorithms, and ways to achieve set goals [5].

In addition, the of Ukrainian National Bar Association has established a working group on the Legal Regulation of Artificial Intelligence. This working group analyzes the most important legal issues concerning the development and use of artificial intelligence, determines the boundaries of its use in various fields, and addresses the protection of personal data collected by AI systems, as well as the rules for their storage and use. The working group contributes to the development of this field and helps ensure the proper protection of human rights when using AI systems [6].

The implementation of such an innovative technology as artificial intelligence into the electoral process undoubtedly has both positive and negative aspects that can significantly impact the entire electoral system of Ukraine.

Among the positive aspects of AI implementation in the electoral system, we can highlight the following:

1) democratization of the electoral process and provision of the possibility of direct participation regardless of the place of stay and the effect of a state of war or emergency;

2) The state can become closer to citizens and, ultimately, represent them more effectively by adhering to the election schedule regardless of special legal regimes;

3) Electronic voting, which has already begun to be implemented in Ukraine, can become a complete innovative technology for a democratic electoral process when combined with artificial intelligence;

4) The implementation of AI elements in the electoral system can address a range of issues related to inclusiveness;

5) It can facilitate the work of election commissions and the Central Election Commission in conducting elections, counting votes, informing voters during the electoral process, and more.

However, concerns about the use of artificial intelligence in politics have existed since the late 2010s. Specifically, issues concerning democracy and the electoral process have intensified with the recent evolution of artificial intelligence.

Regarding the risks and negative consequences, it should be emphasized that this technology creates numerous risks for democracies, as it is also a powerful tool for disinformation, which can provoke tension and lead to election-related conflict, even violence. AI can generate and spread false information. Furthermore, the generalized and analyzed information processed by AI can become

the basis for manipulating public sentiments, as it allows for targeted influence on vulnerable or weak voter categories to "push through" a necessary emotion, opinion, mood, etc. Overall, despite its advantages, artificial intelligence can negatively impact the democratic nature of the electoral process. The development of a "democracy capable of defending itself" should include protection against the use of AI to violate electoral rights and prevent interference in the electoral process.

However, despite the aforementioned risks, artificial intelligence can be beneficial for democracies if proper security measures are applied. For example, specific tools can be used to detect signs of AI-generated content, and methods such as watermarks can be used to clearly indicate that the content was created by artificial intelligence. The EU is currently adapting its legislative framework to eliminate AI-related dangers and promote the use of reliable, transparent, and accountable AI systems. For example, the European Union Parliament approved the Artificial Intelligence Act, which, according to the governing body, "ensures safety and respect for fundamental rights while stimulating innovation" by establishing safeguards for AI and limiting the use of biometric identification. The document examines how the EU AI Act can be implemented to protect the integrity of elections, privacy rights, and freedom of expression from the influence of interference (especially malicious) by AI-supported entities and systems. In particular, it analyzes the implications of the new rules for the integrity of electoral processes and evaluates how the EU intends to regulate AI systems that pose risks to elections. The goal was to provide political guidance to the European Commission and European legislators by offering mitigation measures related to the main identified risks [7]. At the same time, it should be taken into account that not all risks can be detected at the stage of creating new technologies.

Although concerns about the use of artificial intelligence in politics and its impact on the democratic process are not new, they have been exacerbated by the rise of general-purpose AI and generative AI, which is a technological breakthrough. By 2026, 90% of online content could be synthetically created. Although there is no scientific consensus on how to precisely define artificial intelligence, Joint Research Center of the European Commission proposed an operational definition, according to which AI systems are considered software systems designed by humans that identify the most appropriate action to achieve a specific goal by collecting data and processing information obtained from it. These AI systems are typically used to provide personalized recommendations to people based on their previous searches or analysis of online activity. In November 2022, the research company OpenAI made its ChatGPT chatbot available to the public, a generative AI system designed to generate text after a human user inputs a prompt. ChatGPT also belongs to the category of general-purpose AI, which includes AI systems trained on large language models to adapt to a wide range of tasks in various fields. These systems are designed to be capable of learning and adapting to tasks independently, without following strict instructions, and to make inferences from patterns in analyzed data.

Generative AI systems can reproduce and predict similar patterns to create content. Since the release of ChatGPT, many competitors and analogs have emerged. Generative AI solutions capable of generating text, images, and sound have entered the market. It is expected that generative artificial intelligence will become even more powerful in the near future, and text-based video generators will look even more authentic in the future.

In light of the upcoming elections in the USA, there is already a precedent of inaccurate performance by OpenAI's ChatGPT. When asked questions about future elections and potential outcomes, the AI provided quite controversial and inaccurate information. Consequently, the developers have excluded the possibility for this technology to answer any questions related to the electoral process. OpenAI, (developer of ChatGPT), stated: "We have implemented fixes to ensure that ChatGPT will refuse to answer queries about ongoing election results and will direct people to authoritative sources of information, such as the UK Electoral Commission's website." Clearly, answers to questions about future election winners can create a perception of predetermined and known results among the population. [8]

The functioning of these new AI systems is relatively opaque, with information on how data is collected or how systems are trained often being inaccessible. Besides issues of privacy and intellectual property, AI has the potential for bias, manipulation, and misinformation, which poses

risks to societal unity. However, with proper safeguards and transparency rules, AI can become an extremely useful tool for enhancing the democratic process, particularly during elections. [9,10]

As highlighted by UNESCO research, AI has the potential to enhance democratic values, institutions, and processes in various ways, including elections. [11]

AI can be used to educate citizens about democratic principles, whether through gaining knowledge on political issues or becoming familiar with candidates' positions. For example, political recommendation systems could serve as a basis for chatbots that answer citizens' questions about candidates' election programs. Additionally, specially designed AI tools can inform citizens about how a specific candidate's political views have changed over time.

It should also be emphasized that AI cannot replace humans or eliminate jobs under any circumstances. It is merely a tool to facilitate the search, processing, and summarization of large volumes of information. Furthermore, human resources are crucial for monitoring AI operations; no mechanism can function properly without oversight and supervision. AI cannot "feel" the needs of modern humans, but it can help address current issues.

A significant threat today is that AI provides malicious actors with a broad range of methods for influencing public opinion. First, AI can help monitor the information environment and identify new social rifts that could be exploited in the electoral process. AI's network analysis capabilities can also be used for better targeting of audiences and profiling voters, known as political micro-targeting. This could lead to the creation of entire fake websites posing as news outlets.

New AI tools also allow for the generation of images from text or cloning human voices. Deepfake videos are becoming easier to create and increasingly convincing, with text-to-video conversion being termed as a breakthrough in generative AI. Deepfakes pose a huge potential for misinformation (false or inaccurate information) or even disinformation (information intended to deceive), especially through the creation of memes and humorous video content, both of which often go viral online. Politicians are a primary target for deepfakes, as they are an effective mechanism for malicious actors seeking to deceive voters.

Overall, deepfakes pose a serious risk of undermining trust in the information environment. Breakthroughs in generative AI raise concerns about influence campaigns, as now less human and financial resources are needed to conduct large-scale disinformation campaigns. AI systems themselves can generate disinformation. Research has shown that Google's Bard AI tool generates convincing disinformation content in 78 out of 100 tested narratives.

While AI developers are working to make their models more reliable, for example, by conducting red teaming exercises (a process where teams simulate attacks to test security), AI can easily be used to develop and spread harmful narratives online, tailored to the specific context of individual countries. The spread of disinformation can be even more effective with the use of interactive chatbots, which can tailor interactions based on voter group characteristics and adapt manipulation tactics in real time. Generally, AI has a significant manipulative potential, as users may not be able to distinguish between content created by humans and content created by AI.

Researchers have demonstrated the persuasive power of AI, showing that AI-generated messages on various topics were at least as convincing as those created by humans, and users even trust tweets generated by AI more than text written by humans.

Politicians often view letters and correspondence from their constituents as expressions of public opinion on which they can act. The development of AI makes it possible to conduct astroturfing campaigns, where a small group, posing as a genuine wide social group, represents a distorted view of public opinion. For example, AI could be used to create fake correspondence aimed at influencing lawmakers. [12]

AI can both benefit and threaten the democratic nature of elections. EU legislation already includes some rules to address risks associated with the use of AI tools. For example, the EU General Data Protection Regulation (GDPR) and the EU Regulation on the Protection of Data (2018/1725) give

users the right to object to profiling, but also restrict the creation of profiles based on the use of sensitive information. [13,14]

Additionally, the EU is currently adapting its legislative framework to counter the risks of artificial intelligence, particularly concerning democracy. The European Commission launched several legislative initiatives to combat disinformation. Following this, the Code of Practice on Disinformation was adopted, where key online platforms voluntarily agreed to self-regulation standards to combat disinformation. In 2021, the Commission issued guidelines to strengthen the Code of Practice on Disinformation, and in 2022, a new Code of Practice on Disinformation was adopted. It was agreed to implement enhanced transparency measures for political advertising, ensuring more effective labeling, disclosing sponsors, and advertising expenses and display periods, as well as implementing advertising libraries. The Code also aims to expand users' abilities by providing tools for recognizing, understanding, and labeling disinformation and accessing authoritative sources, along with media literacy initiatives.

Separately, the Digital Services Act (DSA) should be mentioned, which came into force in November 2022. According to the DSA, large online platforms must apply a risk-based approach through independent risk management audits. The Code of Practice on Disinformation is recognized by the DSA. Thus, compliance with the Code can be considered an appropriate measure for reducing risk for large platforms. The DSA also addresses concerns regarding micro-targeting of citizens. It bans targeted advertising for minors based on profiling and targeted advertising based on profiling using special categories of personal data, such as political views. It also imposes transparency requirements for online platforms.

Therefore, AI can be a powerful tool to improve content moderation and detect fake news on social media. However, reducing the visibility of content also carries risks of blocking legitimate forms of expression, limiting the distribution of legitimate content, limiting democratic debate, and limiting pluralism during elections. The risk of bias that can arise with AI models can exacerbate these concerns. To address the opacity of platforms and understand their impact on society, the DSA allows verified public interest researchers to access data from large online platforms and thereby increase their accountability to society.[14]

Regarding the implementation and use of AI tools in Ukraine's electoral system, it should be noted that all elements are in the development and exploration stage. Initially, AI could be used in vote counting and the introduction of electronic voting systems. Thus, these elements are being implemented together, as electronic voting requires electronic vote counting. Practical testing of this system (at least at the level of electronic voting) has not yet occurred in Ukraine, meaning we have not had the opportunity to assess potential threats and risks. However, studying foreign experience is a promising direction for further research.

An important and extremely interesting aspect for the domestic legal system is the Artificial Intelligence Act, which adopts a risk-based approach and establishes specific regulatory requirements for high-risk AI systems. In its position on this Act, the European Parliament added to the list of high-risk AI systems those used to influence voters in political campaigns. It also introduced a multi-tiered approach to regulating general-purpose AI. Providers of major models (defined in the Parliament's position as AI systems trained on broad data at scale, designed for general outcomes, and adaptable to a wide range of specific tasks) would need to ensure strong protection of fundamental rights, democracy, the rule of law, An issue of significant interest and importance for the domestic legal system is the Artificial Intelligence Act (AI Act), which introduces a risk-based approach and sets specific regulatory requirements for high-risk AI systems. In its position on this Act, the European Parliament has included AI systems used for influencing voters in political campaigns as high-risk. It has also proposed a multi-tiered approach to the regulation of general-purpose AI. Providers of major models (defined by the Parliament as AI systems trained on broad datasets, designed for general results, and adaptable to a wide range of specific tasks) would need to ensure robust protection of fundamental rights, democracy, the rule of law, health, safety, and the environment. Moreover, generative base models of AI aimed at creating text, images, audio, or video must disclose that the content was generated by AI rather than humans. Additionally, they must be trained and designed to prevent the creation of illegal content. Institutional negotiations are currently ongoing

to finalize the proposed AI Act. Adapting and implementing its norms within the framework of "electronic governance" in Ukraine seems the most effective and promising approach. Since the initiation of e-government, Ukraine has clearly set a course toward implementing innovative and other electronic technologies in leading areas of public life, and these trends will inevitably affect the electoral process. Modern technologies could transform scientific positions and constitutional provisions regarding the impossibility of conducting elections under martial law.

5. Conclusions.

Despite the Russian aggression and the extremely challenging and tense situation across all spheres of public life, Ukraine is actively focused on European integration and the prompt adaptation of domestic legislation to European standards. The electoral sphere will not be an exception. The modern world is constantly evolving, and the implementation of AI in the electoral system could today offer Ukraine positive and necessary solutions to urgent issues, such as engaging frontline defenders in elections or Ukrainian citizens who have had to leave their homes and are currently in various countries around the world. Of course, introducing AI into such a significant sphere carries risks; however, in a constantly changing information environment and with the rapid development of innovative technologies, Ukraine must focus on the use of AI in the electoral system to maintain its status as an information-rich state. It is important to emphasize that, given the ongoing Russian aggression and the active use of AI tools (such as Deepfake), the implementation of AI in Ukraine's electoral system is feasible only with robust protections against interference in electronic voting and the electoral process as a whole.

References:

1. Asirian S. R. (2023) Kroky krain YeS u napriamu zakhystu konstytutsiinykh prav hromadian v epokhu shtuchnoho intelektu [Steps of the EU countries in the direction of protecting the constitutional rights of citizens in the era of artificial intelligence]. Scientific bulletin of Uzhhorod University: series: Law (head. ed.Yu. M. Bysaha), Uzhhorod, V.2, 76, 285–290 [in Ukrainian]

2. Katkova T.H. (2020) Shtuchnyi intelekt v Ukraini: pravovi aspekty [Artificial intelligence in Ukraine: legal aspects]. Law and society. 6, 46–55 [in Ukrainian]

3. Kurakin O.M., Skriabin O.M. (2023) Osoblyvosti pravovoho rehuliuvannia vykorystannia shtuchnoho intelektu v Ukraini [Peculiarities of legal regulation of the use of artificial intelligence in Ukraine]. Bulletin of Kharkiv National University named after V. N. Karazin. "Law" series. 36, 36–42 [in Ukrainian]

4. Frantsuz A., Stepanenko N. ta Shevchenko A. (2023) Problema shtuchnoho intelektu u vyborchomu protsesi [The problem of artificial intelligence in the election process]. Legal Bulletin. 3(9), 71–76 [in Ukrainian]

5. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini: rozporiadzhennia Kabinetu Ministriv Ukrainy [On the approval of the Concept of the development of artificial intelligence in Ukraine: order of the Cabinet of Ministers of Ukraine.] (2020). Government courier, 247 [in Ukrainian]

6. Kornieieva S.R. (2021) Teoretychni pidkhody do vyznachennia poniattia ta pravovoho rehuliuvannia shtuchnoho intelektu [Theoretical approaches to the definition of the concept and legal regulation of artificial intelligence]. Scientific Bulletin of the Uzhhorod National University. Law series, 66, 50Э55 [in Ukrainian]

7. The EU's artificial intelligence act and its impact on electoral processes. URL: https://www.wahlbeobachtung.org/en/the-eus-artificial-intelligence-act-and-its-impact-on-electoral-processes/ [in English]

8. OpenAI's ChatGPT stops answering election questions after giving wrong answers. URL: https://news.sky.com/story/openais-chatgpt-stops-answering-questions-on-election-results-after-wrong-answers-13148929 [in English]

9. AI and Elections – Observations, Analyses and Prospects. URL: https://il.boell.org/en/2022/01/27/ШІ-and-elections-observations-analyses-and-prospects [in English]

10. Smart elections: is AI the Next Wave in Elections Managements? URL: https://www.idea.int/news/smart-elections-ШІ-next-wave-electoral-management [in English]

11. Policy paper on Artificial Intelligence's (AI) Impact on Freedom of Expression in Political CampШІgn and Elections. April 2021. Armin Rabitsch, , Rania Wazir, , and Thomas Treml [in English]

12. How AI puts elections at risk – and the needed safeguards. URL: https://www.brennancenter.org/our-work/analysis-opinion/how-ШІ-puts-elections-risk-and-needed-safeguards [in English]

13. Rehlament Yevropeiskoho parlamentu i rady (YeS) 2016/679 vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zviazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, ta pro skasuvannia Dyrektyvy 95/46/YeS (Zahalnyi rehlament pro zakhyst danykh) [Regulation of the European Parliament and of the Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EC (General Regulation on data protection)]. URL: https://zakon.rada.gov.ua/laws/show/984_008-16 [in Ukrainian]

14. Zakonodavstvo proty dezinformatsii: rol zakonu pro tsyfrovi posluhy v YeS ta perspektyvy dlia Ukrainy [Legislation against disinformation: the role of the law on digital services in the EU and prospects for Ukraine]. URL: https://www.pravda.com.ua/columns/2023/12/7/7432045/ [in Ukrainian]

Oleksii Kurashov,
PhD Candidate, Full-time
Scientific Research Institute of State Building and Local Government of
National Academy of Legal Sciences of Ukraine
E-mail: velocitykh@gmail.com