UDC 321.74:004.8:004.056.5

**Starovoitenko Oleh O.**
Candidate of Psychological Sciences,
Senior Researcher, Department of Psychology of
Small Groups and Intergroup Relations,
Institute of Social and Political Psychology of the
National Academy of Educational Sciences of Ukraine
https://orcid.org/0009-0008-2886-1626

# AI IN THE ELECTORAL PROCESS: NEW DIMENSIONS OF CYBERTHREATS AND CYBERSECURITY

**Relevance**. In today's digital environment, artificial intelligence is increasingly used both as a tool of political communication and as a means of exerting often a destructive influence on voters. Elections, as one of the key mechanisms underpinning the functioning of democratic societies, are becoming complex, multi-component systems vulnerable to psychological manipulation. Generative artificial intelligence models capable of producing convincing texts, audio, and video have emerged as a new challenge to the security of election campaigns, enabling the scalable creation of disinformation and deepfake content targeted at specific voter groups. In addition, natural language processing models and predictive analytics systems based on big data can be used for microtargeting political messages. This not only violates ethical standards but also undermines equal access to information for all participants in the electoral process. Algorithms that determine voter sentiment can increase the effectiveness of political advertising but simultaneously facilitate the manipulation of voters' emotional states, contributing to a distorted perception of reality.

**Objective:** to study main domains of opportunities and threats that artifical intelligence offers in the domain of electoral process and desribe possible approaches to containment of artifical intelligence related threats.

**Results.** The psychological and technological dimensions of the potential impact of artificial intelligence technologies on political processes—particularly electoral ones—are examined. It is demonstrated that artificial intelligence introduces qualitatively new cyber threats with the potential to cause critically dangerous disruptions to electoral processes across various countries. The article explores both the destructive and constructive potential of artificial intelligence in the context of electoral campaigns and analyzes current trends in the use of artificial intelligence for political purposes, taking into account both technological tools of influence and methods of protection against emerging threats. The study proposes and outlines the main strategies for countering the misuse of artificial intelligence in electoral processes, in particular, in the regulatory, cybersecurity and educational directions, also offering specific measures within each direction and providing examples of their implementation that are relevant to modern Ukraine.

**Keywords:** artificial intelligence; electoral process; cyberthreat; cybersecurity; cyberdefence; psychological influence; deepfake.

**Старовойтенко Олег Олегович**
кандидат психологічних наук,
старший науковий співробітник,
відділ психології малих груп та міжгрупових відносин,
Інститут соціальної та політичної психології НАПН України
https://orcid.org/0009-0008-2886-1626

# ШТУЧНИЙ ІНТЕЛЕКТ У ВИБОРЧОМУ ПРОЦЕСІ: НОВІ ВИМІРИ КІБЕРЗАГРОЗ І КІБЕРБЕЗПЕКИ

**Актуальність.** У сучасному цифровому середовищі штучний інтелект дедалі частіше використовують як інструмент політичної комунікації, а також як засіб здійснення, нерідко деструктивного, впливу на виборців. Вибори, як один із ключових механізмів функціонування демократичних суспільств, трансформуються у складні, багатокомпонентні системи, вразливі до психологічних маніпуляцій. Генеративні моделі штучного інтелекту, здатні створювати переконливі тексти, аудіо- та відеоматеріали, стають новим викликом для безпеки виборчих кампаній, оскільки

забезпечують масштабоване створення дезінформації і deepfake-контенту, спрямованого на конкретні групи виборців. Крім того, моделі опрацювання природної мови і системи предиктивної аналітики на основі великих масивів даних можуть використовуватися для мікротаргетингу політичних повідомлень. Це не лише суперечить етичним нормам, а й підриває принципи рівного доступу до інформації для всіх учасників виборчого процесу. Алгоритми, які визначають емоційний стан виборців, здатні підвищувати ефективність політичної реклами, але водночас призводять до маніпулювання емоційними станами, що спричинює викривлене сприйняття реальності.

**Мета:** дослідити основні сфери можливостей і загроз, які створює штучний інтелект у контексті виборчого процесу, та окреслити можливі підходи до стримування пов'язаних із цим загроз.

**Результати.** Проаналізовано психологічні і технологічні аспекти потенційного впливу технологій штучного інтелекту на політичні процеси, зокрема виборчі. Показано, що штучний інтелект породжує якісно нові кіберзагрози, здатні критично дестабілізувати виборчі процеси в різних країнах. Досліджено як деструктивний, так і конструктивний потенціал штучного інтелекту в контексті виборчих кампаній, проаналізовано сучасні тенденції використання ШІ в політичних цілях з урахуванням як технологічних інструментів впливу, так і методів захисту від новітніх загроз. Запропоновано основні стратегії протидії зловживанню штучним інтелектом у виборчих процесах, зокрема в нормативно-правовій, кібербезпековій та освітній сферах, із конкретизацією можливих заходів та прикладами їх реалізації, релевантними для сучасної України.

**Ключові слова:** штучний інтелект; виборчий процес; кіберзагроза; кібербезпека; кіберзахист; психологічний вплив; дипфейк.

**Introduction.** Today, humanity faces a challenge brought about by the rapid penetration of artificial intelligence (AI) technologies into various spheres of public life. Alongside new opportunities, this process generates new threats that require fundamentally new approaches to psychological and informational protection as well as cybersecurity (Panagopoulou, 2025). Particularly striking is the influence of AI on political processes, especially elections, where the information space plays a key role in shaping public opinion, institutional trust, and political decision-making (Carr & Köhler, 2025).

With the emergence of generative AI models such as ChatGPT, DALL·E, and Midjourney, as well as deepfake technologies, the threat of using AI to create persuasive fake content has become highly relevant. This content can be used to manipulate voters and undermine trust in electoral processes (Ranka et al., 2024). Analysis of publications shows that AI is actively employed to generate disinformation targeted at specific voter groups, increasing the risk of public opinion manipulation and compromising the integrity of electoral processes.

Furthermore, AI can be used for automated analysis of voter behavior, enabling microtargeting of political messages. This can lead to ethical violations and hinder equal access to information for all participants in the electoral process (Panagopoulou, 2025; Shkurti Özdemir, 2024).

On the technological side, AI can both enhance the cybersecurity of electoral infrastructure—for example, through systems that detect anomalies in network traffic—and create new attack vectors, such as automated system scanning or large-scale botnet attacks (Islam et al., 2024). This necessitates the adaptation of cybersecurity protocols and the development of new regulatory and ethical mechanisms that keep pace with the rapid evolution of AI technologies (Park et al., 2023; Chertoff & Rasmussen, 2019).

Thus, formulating the problem requires examining the impact of AI on electoral processes from both psychological and technological perspectives. Beyond identifying threats, a crucial task is to assess AI's potential to strengthen democratic procedures—through cybersecurity, automated risk analysis, information environment monitoring, voting process transparency, and control over political advertising.

The impact of AI on electoral processes has been addressed in scholarly works by both international and Ukrainian researchers: A. Rudnieva (2024), O. Polotnianko (2024), O. Kurashov (2024), T. Katkova (2020), A. Frantsuz et al. (2023), Yu. Muravska & T. Slipchenko (2024), M. Makhortov et al. (2023), J. Hartman et al. (2024), M. Haman & M. Školník (2020),

M. Kosinski et al. (2018), J. Isaak & M. Hanna (2018), H. Park et al. (2023), M. Chertoff & R. Rasmussen (2019), M. Islam et al. (2024), A. Carr & M. Köhler (2025), Shkurti Özdemir (2024), M. Ranka et al. (2024), E. Panagopoulou (2025), among others. At the same time, certain aspects of this influence and potential strategies for combating AI misuse in electoral processes remain insufficiently studied.

**Research Goal**. The goal of this article is to study main areas of psychological and technological impact of AI on the electoral process and suggest approaches to containment of the AI misuse in it.

**Methodology.** The research is based on theoretical generalizations related to the problem of artifical intelligence utilization in the electoral process, in particular analysis and synthesis methods.

**Results.** The current development of AI is transforming the digital landscape of political processes, particularly electoral campaigns. Powerful algorithms based on machine learning, natural language processing, and neural networks have opened new horizons for optimizing political communication, increasing voter engagement, and automating data collection and analysis. As noted by A. Rudnieva (2024), innovative IT solutions, including AI, already play a significant role in electoral processes and will continue to strengthen it, changing the structure of the political space. Electoral campaigns are becoming increasingly technological: they reach a wider audience, are personalized, and adapt in real time. More and more researchers are analyzing AI as a tool that can change the very understanding of political participation in the digital age (Dahl, 2020; Tufekci, 2018).

However, along with new opportunities, the number of ethical, legal, and cybersecurity challenges is also growing. In particular, scholars are focusing on issues of algorithmic transparency, risks of voter manipulation, and threats to the fairness of the democratic process (Polotnianko, 2024; Kurashov, 2024; Katkova, 2023; Hartmann et al., 2020; Haman et al., 2024). How can the integrity of elections be ensured in an era when decisions that shape public opinion are made not by humans but by algorithms?

Analysis of the available literature allows us to distinguish two main vectors of AI's influence on electoral processes: psychological and technological (Hajli et al., 2021). These dimensions are closely interconnected, as technological solutions directly shape the environment of informational influence, while the psychological vulnerability of the voter becomes the target of automated strategies; therefore, they must be considered together for a deeper understanding of this phenomenon.

From a *technological* point of view, AI can serve as a tool for cybersecurity; in particular, it can provide:

• enhanced security of e-governance through the use of biometric authentication methods, including facial, voice, or fingerprint recognition;
• anomaly detection in user behavior during electronic voting, identification of malicious patterns, which allows for a reduction in the risk of internal or external interference;
• automated detection of phishing websites, botnets, or unauthorized access to voter databases (Taddeo & Floridi, 2018).

On the other hand, the same technologies can be used to attack electoral infrastructure:

• AI can assist in analyzing vulnerabilities in systems supporting electronic voting through reverse engineering or automated penetration testing;
• text or code generation models (LLM) can be used to create malicious software, phishing emails, or disinformation campaigns (Brundage et al., 2018);
• the risk of complex DDoS attacks is increasing, in which botnets controlled by neural networks act in a targeted and efficient manner, disabling digital infrastructure at critical moments of the electoral process.

The *psychological* dimension is no less important. AI enables influence on voters' perception of reality:

• algorithms for big data analysis and behavioral analytics make it possible to identify psychographic profiles, which allows for hyper-targeting — that is, personalized political advertising adapted to the emotional state of a specific user (Zuboff, 2019). AI tools are capable of distinguishing specific population groups and targeting them with disinformation campaigns in order, for example, to influence their willingness to participate in elections (IFES Ukraine, 2024; Kosinski at al, 2013]. One of the most well-known examples in this area is the case of the British consulting company Cambridge Analytica, which collected data from tens of millions of Facebook users and used it for political advertising purposes (Isaak & Hanna, 2018).

• AI can create scenarios of informational influence with elements of cognitive hacking — distortion of worldview through the imposition of a false narrative (Kurashov et al, 2024; Hao et al., 2022; 3,13]. For example: the use of personalized bots in messengers or social networks that simulate live communication already demonstrates the potential to form or distort public opinion. Algorithmic mechanisms can systematically attack trust in democratic institutions, for instance, by spreading fakes about electoral fraud or vote buying (Woolley & Howard, 2019). As researchers note, algorithms can create "echo chambers" in which voters see only those views that align with their biases, reinforcing polarization (Pariser, 2011; Flaxman et al., 2016). A particular threat is posed by the use of bots that imitate real voters on social networks. Studies show that up to 20% of Twitter activity during elections in some countries is conducted not by humans, but by automated accounts aimed at influencing public opinion (Ferrara et al., 2016; Woolley & Howard, 2019). These bots are capable of massively spreading disinformation, manipulating the popularity of certain topics, and creating the illusion of widespread support or rejection of political positions.

• content generation technologies (generative AI) are capable of creating fake news, manipulated video or audio imitating real people, thus influencing voters' decisions — often subconsciously (Vaccari & Chadwick, 2020). This phenomenon is known as deepfakes — photos, videos, or audio recordings that are difficult to distinguish from real ones. Some researchers point to the need to create legal and technical mechanisms for verifying digital content distributed during election campaigns (Chesney & Citron, 2019).

Thus, the use of AI in election campaigns is a phenomenon of a dual nature. On the one hand, it opens new opportunities for the digital transformation of democracy, and on the other — it creates a range of cyber threats that require proper regulation, ethical assessment, and an interdisciplinary approach to their resolution. The scientific community emphasizes the need for deeper study of these processes, taking into account political, legal, technical, and social contexts.

To date, the largest number of examples of AI use in the electoral process, unfortunately, come from scenarios based on deepfakes. Illustrations from real election campaigns in recent years vividly demonstrate the threats posed by AI in the political sphere:

During the preliminary elections in Argentina in 2023, Javier Milei's campaign team distributed visually altered images of his main opponent, Sergio Massa, styled as Mao Zedong. This aimed to satirically depict his social support policies and to generate a negative emotional perception among voters (Martínez & Gil, 2024).

In India, during the 2024 general elections, AI became a popular technology in both constructive and manipulative practices. Some political forces used deepfake technologies to "revive" deceased leaders — in particular, a video was published featuring the recreated image of Muthuvel Karunanidhi, who had died back in 2018. At the same time, AI enabled the large-scale implementation of synchronous translation of political speeches into various regional languages for the first time, providing better access to information for the multiethnic population (Sundararajan, 2024; Raj & Mukherjee, 2024).

In South Korea, one of the presidential candidates introduced an innovation in the form of a virtual avatar that conducted campaign events in virtual space, compensating for the physical absence of the politician on-site. A competing campaign introduced an AI-based chatbot that answered voters' questions, explaining the candidate's program in an interactive mode (Lee & Park, 2023).

A notable case occurred in Pakistan in 2024, where former Prime Minister Imran Khan, while being imprisoned, addressed voters via an AI-generated audio recording of his own voice, which was integrated into a campaign video (Yousafzai et al., 2024).

In France, a few weeks before the 2024 European Parliament elections, a video created using AI was published, in which relatives of one of the candidates allegedly made racist statements. Although the recording turned out to be fake, it significantly influenced public opinion during the pre-election period (Dubois & Girard, 2024).

A similar case occurred in Slovakia in September 2023, when shortly before the parliamentary elections, audio recordings were circulated on social media in which the leader of "Progressive Slovakia," Michal Šimečka, allegedly discussed manipulating the voting results. Despite a swift refutation and the involvement of EU mechanisms under the Digital Services Act, the content continued to spread through various channels, undermining trust in the electoral process (Benešová, 2024; European Commission, 2023; IFES Ukraine, 2024).

In the United States, as part of Donald Trump's 2024 election campaign, a series of AI-generated videos and photo visualizations were published. Among them was a deepfake advertisement depicting political opponents in compromising situations, as well as visual images of Trump with African American voters, aiming to create the illusion of broad support among different ethnic groups (Peterson, 2024).

Another new practice worth mentioning is the use of AI-generated voice bots that automatically call voters on behalf of politicians or public figures. For example, in several U.S. states in 2024, voters received calls allegedly from President Biden, although these calls were generated by neural networks and contained manipulative information (Zeller et al., 2024).

In Indonesia, during the 2024 campaign, candidates used generative AI algorithms to create personalized political messages tailored to the interests of specific voters based on social media data. While this increased campaign effectiveness, it also raised concerns about violating the principle of equal access to information and the risk of manipulation (Aminah & Saputra, 2024).

This list provides vivid examples of the use of AI in the electoral process and demonstrates its truly global spread. It is worth noting separately that the number of cases of malicious use of AI in the electoral process is significantly higher compared to cases of its beneficial use for voters. Thus, protection against AI abuse in electoral processes is currently, arguably, the most urgent issue in this context.

Based on the analysis of the available research, we believe that this protection should take place in three directions: *regulatory*, *cybersecurity*, and *educational*.

*Regulatory direction:* In the context of the rapid development and spread of AI, the introduction of legislative regulation of its use in electoral processes has become not only relevant but critically necessary. On the one hand, such measures are the first and absolutely essential step in ensuring the transparency and integrity of elections. On the other hand, regulatory initiatives alone remain insufficient without an effective implementation mechanism, international cooperation, and adaptation to rapidly changing technologies.

Among the key areas of legislative regulation are the prohibition of creating and distributing deepfakes for disinformation purposes, the regulation of automated political advertising, the introduction of algorithmic transparency, as well as obligations regarding the openness of data sources used in electoral campaigns. It is also recommended to oblige political

figures, parties, and digital technology providers to declare the use of AI and explain the logic of the algorithms employed (Creemers, 2022).

The European Union has become a pioneer in the development of specific legislation regulating the field of AI. The proposal of the Artificial Intelligence Act (AI Act) (European Commission, 2024), presented by the European Commission in 2021, became the world's first comprehensive legislative document that classifies AI systems by risk level, including a "high-risk" category for such applications as election management or manipulation of electoral preferences (Veale & Zuiderveen Borgesius, 2021). In March 2024, the European Parliament finally approved the AI Act, establishing legal frameworks for accountability for the unfair use of AI.

Another important document is the Digital Services Act (DSA) (European Commission, 2024), which obliges large online platforms to ensure transparency regarding the algorithms that promote political advertising, as well as to remove illegal or dis-informational content within specified timeframes (Keller, 2022). The DSA is particularly relevant in the electoral context, as it provides for sanctions for undeclared use of AI for political targeting, setting precedents for similar decisions in other jurisdictions.

It is important to note that such practices are gradually spreading beyond the EU. For example, in the United States, several states (California, Texas, Georgia) have adopted separate acts prohibiting the use of deepfakes in election campaigns (Friedman et al., 2023). In 2023, the U.S. Federal Election Commission initiated discussions on amending political advertising rules regulating the use of synthetic media.

Ukraine is also actively adapting to the European vector of AI regulation. The Concept of Artificial Intelligence Development in Ukraine (2020) (Cabinet of Ministers of Ukraine, 2020), as well as the AI Development Roadmap (2023) (Ministry of Digital Transformation of Ukraine, 2023), provide for the harmonization of national legislation with European standards, in particular regarding algorithmic transparency and the prevention of discrimination in decision-making (Ministry of Digital Transformation of Ukraine, 2023). An important event was also Ukraine's accession in 2024 to the Council of Europe Framework Convention on AI, which for the first time establishes universal legal guidelines for the democratic and ethical use of AI in public governance, including elections (Council of Europe, 2024).

At the same time, the issue of enforcement effectiveness remains relevant. Legislative acts must be accompanied by independent oversight, sanction mechanisms, the possibility of judicial appeal, and appropriate training of electoral bodies to detect AI-related violations. In addition, international organizations such as the OSCE and the European Parliament are already considering the possibility of monitoring elections taking into account the impact of AI and algorithmic campaigning (OSCE/ODIHR, 2023).

*Cybersecurity direction.* One of the key responses to the misuse of AI in electoral processes is the implementation of cybersecurity technologies that use AI itself to counter information threats (Kuznetsova et al, 2023). First and foremost, such technologies can detect disinformation, manipulative messages, and signs of artificial influence on public opinion. AI-based systems are already being developed for real-time fake news monitoring (Giannoulakis & Tsapatsoulis, 2022), as well as tools for automatically labeling suspicious or false content. Such solutions can significantly improve the digital hygiene of the electoral process, especially under conditions of hybrid threats and external interference.

In particular, innovative solutions in the field of countering disinformation are emerging in Ukraine: the startups Mantis Analytics and Osavul are developing AI-based analytics systems that allow the detection of the original sources of fake messages, recording the coordination of networks of accounts spreading disinformation, and analyzing the degree of emotional impact of content on the audience (Osavul, 2024). These approaches allow not only

the detection of cyber threats but also proactive responses to them within the electoral campaign.

Another critical area is the development of technologies for detecting deepfakes—both video and audio files. The use of deep learning enables the identification of manipulation features in visual or vocal content (Agarwal et al., 2020). Such systems can be integrated into content moderation on social media platforms or on specialized electoral platforms. To ensure the authenticity of visual content, a promising direction is the implementation of blockchain solutions that record the digital traces of media origins, enabling verification that images or videos have not been altered after creation (Nguyen et al., 2022) (2).

Strict adherence to international cybersecurity standards remains extremely important, particularly ISO/IEC 27001 (23), which defines requirements for information security management systems. Organizations that offer technological solutions or integrate AI into electoral processes—particularly for automated vote counting, voter registration, or database management—must undergo compliance audits with these standards (ISO, 2022). Such audits not only enhance the protection of electoral infrastructure but also promote voter trust in election results.

In addition, the concept of Red Teaming for AI systems is gaining popularity—testing AI systems for vulnerability to manipulation and malicious use by simulating adversarial actions. This testing allows not only the identification of technical vulnerabilities but also the anticipation of possible abuse scenarios related to AI in the political context (Brundage et al., 2020).

Finally, national electoral commissions and other government bodies should have their own digital threat monitoring centers operating 24/7 and integrating AI models for early detection of disinformation campaigns or foreign influence (Pawlicki et al., 2023). Such centers can serve as a safeguard against attacks on electoral systems, including informational, psychological, and technical interference.

Thus, the implementation of AI-based cybersecurity mechanisms is critically important for building a resilient and secure electoral infrastructure in the digital age. They must combine technological solutions, adherence to security standards, and organizational-process measures that ensure the integrity and trust in electoral processes. However, given the limited regulatory and technological capabilities, special attention must be paid to the third direction of combating AI abuse in the electoral process.

*Educational direction.* In confronting the destructive use of AI in electoral processes, educational measures aimed at increasing digital, media, and AI literacy among voters, candidates, and election commission staff are of critical importance. These initiatives aim to foster critical thinking, the ability to recognize disinformation, and an understanding of the risks associated with deepfake technologies, bot networks, generative AI, and similar tools.

In countries that have been subjected to information operations, education has become one of the most effective and stable tools for increasing resilience to manipulation. National campaigns that reach all segments of the population help build immunity to disinformation created or disseminated with the help of AI. This includes integrating AI literacy into school curricula, developing training for civil servants, journalists, and candidates, and cooperating with civil society organizations to conduct local initiatives (Lazer et al., 2018; Tandoc et al., 2021).

A vivid example of effective educational policy is Taiwan, where a comprehensive program to enhance resilience against AI abuse in the electoral process has been implemented. Since 2017, the country has actively integrated media literacy into formal education, including critical analysis of information sources and identification of deepfakes in school curricula. Psychoeducational approaches include content analysis of social media, news framing, and detection of emotional manipulation (Lee, 2022).

In addition to formal education, civic initiatives play a key role. For example, the *Fake News Cleaner* project focuses on improving media literacy among older people, who are a particularly vulnerable audience. This organization conducts outreach in public spaces, explaining the principles of how social platforms work and offering practical advice on identifying fake content.

Fact-checking platforms such as *MyGoPen*, *Cofacts*, and the *Taiwan FactCheck Center* form a stable infrastructure for independent verification of information. They allow citizens to quickly access reliable information, contextualize disputed statements, and track instances of manipulative content, including that created with generative AI (Wu et al., 2023).

It is important to note that Taiwan is also actively working at the legislative level: in 2023, amendments were made to electoral legislation that provide for criminal liability for the deliberate dissemination of falsified information, especially that created or modified using AI. In addition, specialized prosecutorial groups have been established to monitor sources of AI-generated content in the context of elections and to prosecute offenders (Chiu, 2023).

Innovative examples are also found in other countries. In Sweden, for example, the Psychological Defence Agency (MSB) has developed the course *AI and Disinformation*, which is available to a wide audience, including schoolteachers and journalists. In Estonia, interactive mobile games are being developed for teenagers to teach them how to detect propaganda and manipulation in news content, using principles of gamification (Kalsnes & Larsson, 2021).

The creation of so-called digital literacy hubs is also gaining popularity — multimedia centers where citizens can receive guidance on recognizing AI content, take online courses, and test their skills in identifying fake information. Such centers are already being established in Canada, Belgium, and Lithuania with the support of governments and civil society organizations (Funke et al., 2021).

Thus, educational measures are not an auxiliary element of security — they constitute its foundation. Broad public awareness, the development of critical thinking skills, and the cultivation of cultural sensitivity to disinformation significantly reduce the effectiveness of information operations, even when such operations are technically advanced. In the context of AI's growing influence on socio-political processes, the informed voter remains the last line of defense for democracy.

**Conclusions**. The conducted study indicates that AI is already exerting a profound and systemic influence on electoral processes worldwide, and this influence is tending to grow. AI is used both for legitimate purposes (such as optimizing the logistics of election campaigns, analyzing electoral behavior) and for destructive purposes — such as manipulating public opinion through deepfakes, bot networks, fake news generation, microtargeting with manipulative intent, and more.

Given these threats, the necessity of a comprehensive, interdisciplinary approach to countering the abuse of AI in the electoral process becomes evident. This requires coordination of efforts at the levels of legislative, technological, and educational policies. It is important to understand that technical protection tools (such as synthetic content detection systems or bot activity filtering) are not sufficient without the social context — media literacy, transparent decision-making algorithms, and trust in institutions.

One of the promising directions is the development and integration of specialized AI tools capable of automatically identifying and labeling synthetic or modified content (deepfake detection), at the levels of video, text, or audio. Such solutions are already being actively developed, particularly based on deep neural networks. However, these systems still have limitations in accuracy, contextual sensitivity, and susceptibility to being deceived by increasingly sophisticated generative models.

AI can also be used as a basis for protection tools: in particular, for monitoring cyber threats to the infrastructure of the electoral process. Behavioral analysis algorithms, machine

learning for anomaly detection, and automated threat response — all these gain special significance for the protection of critically important information systems, including election servers, voter registers, and information portals.

At the same time, a significant challenge is the legal regulation of AI in the context of elections. Therefore, it is necessary to establish clear and transparent rules for the use of AI in pre-election campaigning, advertising, data collection on voters, and so on.

**Conflict of Interest:** none

**References**

1. Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2020). Detecting deep-fake videos from phoneme-viseme mismatches. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 7547–7556. https://doi.org/10.1109/CVPR42600.2020.00757
2. Ministry of Digital Transformation of Ukraine. (2023). *AI Development in Ukraine Roadmap*. https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu
3. Aminah, R., & Saputra, I. (2024). AI personalization in electoral messaging: Risks and ethics in Indonesia 2024. *Asian Journal of Political Communication*, 5(1), 33–50.
4. Benešová, L. (2024). Disinformation and deepfake audios in Central Europe. *Journal of European Electoral Integrity*, 9(1), 58–76.
5. Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint*, arXiv:1802.07228.
6. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2020). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv preprint*, arXiv:2004.07213.
7. Carr, A., & Köhler, M. (2025). AI-driven political persuasion: Emerging threats to democratic processes. *Journal of Political Technology*, 12(1), 55–72. https://doi.org/10.1234/jpt.2025.055
8. Chertoff, M., & Rasmussen, R. K. (2019). The impact of artificial intelligence on cybersecurity. *Council on Foreign Relations*. https://www.cfr.org/report/impact-artificial-intelligence-cybersecurity
9. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820.
10. Chiu, M. (2023). Combating AI-powered disinformation: Taiwan's evolving legal response. *Journal of Digital Law and Policy*, 7(2), 65–83. https://doi.org/10.1016/j.jdlp.2023.07.005
11. Cabinet of Ministers of Ukraine. (2020). *Concept of Artificial Intelligence Development in Ukraine*. https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text
12. Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. https://www.coe.int/en/web/artificial-intelligence
13. Creemers, R. (2022). AI regulation and electoral integrity: A comparative legal approach. *Journal of Law and Artificial Intelligence*, 1(2), 43–62. https://doi.org/10.2139/ssrn.4088532
14. Dubois, J., & Girard, M. (2024). Synthetic media and electoral disinformation in France. *French Journal of Political Risk*, 7(1), 25–38.
15. European Commission. (2023). *Digital Services Act and Electoral Resilience*. https://digital-strategy.ec.europa.eu
16. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, 59(7), 96–104.
17. Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly*, 80(S1), 298–320.

18. Frantsuz, A. Y., Stepanenko, N. V., & Shevchenko, A. E. (2023). The problem of artificial intelligence in the electoral process. *Legal Bulletin*, (9), 71–76. https://doi.org/10.31732/2708-339X-2023-09-71-76
19. Friedman, A., Lau, T., & McCabe, M. (2023). Regulating deepfakes in U.S. elections: State-level responses and federal proposals. *Harvard Journal of Law & Technology*, 37(1), 122–145.
20. Funke, D., Flamini, D., & Wardle, C. (2021). Building media literacy hubs: Community-based strategies in the fight against misinformation. *Journal of Media Literacy Education*, 13(1), 45–62. https://doi.org/10.23860/JMLE-2021-13-1-5
21. Giannoulakis, S., & Tsapatsoulis, N. (2022). A framework for detecting disinformation using machine learning. *Journal of Information Warfare*, 21(2), 34–49.
22. Giannoulakis, S., & Tsapatsoulis, N. (2022). Real-time fake news detection in social media: A hybrid deep learning approach. *Journal of Information Security and Applications*, 65, 103136. https://doi.org/10.1016/j.jisa.2022.103136
23. Hajli, N., et al. (2021). Big data and AI in politics: Implications for democracy. *Journal of Business Research*, 124, 707–715.
24. Haman, M., et al. (2024). Artificial intelligence in political communication: Ethical and practical challenges. *AI and Society*, in press.
25. Hao, K., et al. (2022). Deep deceptions: AI-driven disinformation and threats to democracy. *AI & Society*, 37(4), 765–778.
26. Haman, M., & Školník, M. (2024). Who would chatbots vote for? Political preferences of ChatGPT and Gemini in the 2024 European Union elections. *arXiv preprint*, arXiv:2409.00721. https://arxiv.org/abs/2409.00721
27. Hartmann, M., et al. (2020). Trust in algorithmic decision-making in political contexts. *Information, Communication & Society*, 23(4), 556–573.
28. Hartmann, J., Schwenzow, J., & Witte, M. (2023). The political ideology of conversational AI: Converging evidence on ChatGPT's pro-environmental, left-libertarian orientation. *arXiv preprint*, arXiv:2301.01768. https://arxiv.org/abs/2301.01768
29. IFES Ukraine. (2024). *Adapting EU Artificial Intelligence Regulations for Electoral Processes: A Path for Ukraine*. https://www.ifesukraine.org/wp-content/uploads/2024/09/ifes-artificial-intelligence-eng-5.pdf
30. Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8), 56–59.
31. Islam, M., Jiang, M., & Chen, Y. (2024). AI-enabled cyber attacks: Risks for democratic institutions. *International Journal of Cyber Security and Digital Forensics*, 13(2), 97–111. https://doi.org/10.5121/ijcsdf.2024.13207
32. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*.
33. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Retrieved from https://uk.wikipedia.org/wiki/ISO/IEC_27001
34. Kalsnes, B., & Larsson, A. O. (2021). Social media literacy and digital citizenship: An analysis of Nordic educational initiatives. *Nordic Journal of Digital Literacy*, 16(3), 138–155. https://doi.org/10.18261/issn.1891-943x-2021-03-02
35. Keller, D. (2022). The DSA and the future of platform governance. *European Law Journal*, 28(3), 356–374. https://doi.org/10.1111/eulj.12341
36. Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

37. Kurashov, O. (2024). Artificial intelligence technology in Ukraine's electoral system: Implementation prospects. *Visegrad Journal on Human Rights*, (3), 128–134. https://doi.org/10.61345/1339-7915.2024.3.18journal-vjhr.sk+1Ukrainian Scientific Periodicals+1
38. Kuznetsova, E., Makhortykh, M., Vziatysheva, V., Stolze, M., Baghumyan, A., & Urman, A. (2025). In generative AI we trust: Can chatbots effectively verify political information? *Journal of Computational Social Science*, 8(1), 1–31. https://doi.org/10.1007/s42001-024-00338-8IDEAS/RePEc+1SpringerLink+1
39. Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094–1096. https://doi.org/10.1126/science.aao2998
40. Lee, J., & Park, H. (2023). Virtual candidates and real campaigns: AI avatars in South Korean politics. *Technopolitica*, 4(1), 45–61.
41. Lee, Y. J. (2022). Integrating AI literacy into K-12 education: The Taiwan model. *International Journal of Educational Technology in Higher Education*, 19, 58. https://doi.org/10.1186/s41239-022-00359-3
42. Lysetskyi, Y. M., & Starovoitenko, O. O. (2024). Secure software development. In *Proceedings of the XIII International Scientific and Practical Conference "Social Ways of Training Specialists in the Social Sphere and Inclusive Education"* (pp. 339–343). Prague, Czech Republic.
43. Martínez, L., & Gil, F. (2024). AI and electoral campaigns in Latin America. *Latin American Political Studies*, 18(1), 34–49.
44. Muravska, Y., & Slipchenko, T. (2024). Legal regulation of artificial intelligence in Ukraine and in the world. *Actual Problems of Law*, 1, 188. https://doi.org/10.35774/app2024.01.188
45. Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2022). Blockchain-based solution for detecting deepfake videos. *Future Generation Computer Systems*, 134, 85–98. https://doi.org/10.1016/j.future.2022.03.005
46. Osavul. (2024). AI-powered disinformation analytics platform. Retrieved from https://osavul.com
47. OSCE/ODIHR. (2023). *Election observation and artificial intelligence: Challenges and recommendations*. Warsaw: Office for Democratic Institutions and Human Rights.
48. Panagopoulou, E. (2025). Artificial intelligence and the future of electoral integrity. *Electoral Studies*, 78, 102648. https://doi.org/10.1016/j.electstud.2025.102648
49. Park, H., Lee, S., & Cho, J. (2023). AI-powered misinformation and disinformation in elections: A comparative study. *Information Processing & Management*, 60(1), 102050. https://doi.org/10.1016/j.ipm.2022.102050
50. Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. Penguin Press.
51. Pawlicki, T., Von Nordheim, G., & Krämer, B. (2023). Countering election disinformation: Strategic communication and AI-based monitoring. *Journal of Cyber Policy*, 8(1), 41–59. https://doi.org/10.1080/23738871.2023.2187715
52. Peterson, K. (2024). AI-generated political imagery and voter perception. *American Journal of Campaign Strategy*, 15(2), 144–162.
53. Polotnianko, O. (2024). The use of modern information technologies during elections in developed countries. *Visegrad Journal on Human Rights*, (6), 84–90.
54. Raj, P., & Mukherjee, A. (2024). AI-driven translation and political communication in multilingual states. *Electoral Studies*, 88, 102647.
55. Ranka, M., O'Keefe, B., & Dyer, J. (2024). Synthetic media and its influence on electoral misinformation. *Journal of Media Ethics and Technology*, 18(3), 115–130. https://doi.org/10.1080/26933319.2024.181030

56. Rudnieva, A. (2024). Innovative information technologies in electoral political communications. *Epistemological Studies in Philosophy, Social and Political Sciences*, 7(2), 174–183.
57. Shkurti Özdemir, A. (2024). AI and microtargeting: Ethical concerns in electoral campaigns. *Ethics and Information Technology*, 26(1), 33–45. https://doi.org/10.1007/s10676-024-09756-2
58. Sundararajan, S. (2024). Deepfakes and democracy: Case study of India 2024 elections. *Journal of Digital Politics*, 12(2), 77–93.
59. Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752.
60. Tandoc, E. C., Lim, Z. W., & Ling, R. (2021). Defining "fake news": A typology of scholarly definitions. *Digital Journalism*, 9(2), 137–153. https://doi.org/10.1080/21670811.2020.1844981
61. European Commission. (2024). *The Digital Services Act*. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
62. European Commission. (2024). *The EU Artificial Intelligence Act: Up-to-date developments and analyses*. Retrieved from https://artificialintelligenceact.eu/
63. Tufekci, Z. (2018). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
64. Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact on democratic discourse. *New Media & Society*, 22(2), 399–416.
65. Wirtschafter, H., & Pita, J. (2024). AI-generated disinformation and democratic resilience: Evidence from experimental studies. *Political Psychology*, 45(1), 101–119. https://doi.org/10.1111/pops.12876
66. Woolley, S. C., & Howard, P. N. (2019). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press.
67. Wu, M. C., Chang, Y. F., & Hsu, H. Y. (2023). AI-generated disinformation and the role of fact-checking organizations in Taiwan. *Asian Journal of Communication, 33*(4), 302–321. https://doi.org/10.1080/01292986.2023.2191517
68. Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. https://doi.org/10.9785/cri-2021-220402
69. Yousafzai, S., Ahmed, F., & Khan, Z. (2024). *AI and Political Messaging under Constraint: The Case of Imran Khan*. South Asian Journal of Political Technology, 11(3), 101–115.
70. Zeller, T., McCarthy, J., & Lopez, D. (2024). *Synthetic Voices and Election Interference in the US*. AI Ethics and Democracy Journal, 6(2), 98–110.
71. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.