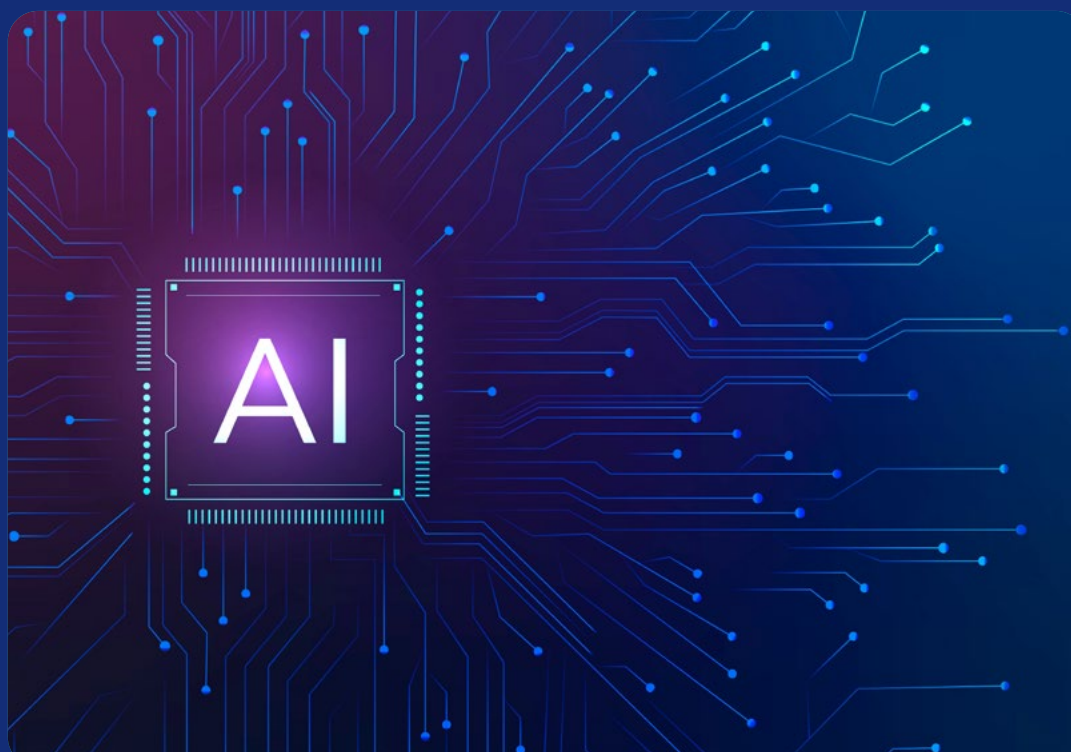
Adapting EU Artificial Intelligence Regulations for Electoral Processes: A Path for Ukraine

IFES Ukraine | September 2024



Adapting EU Artificial Intelligence Regulations for Electoral Processes: A Path for Ukraine

The regulation of Artificial Intelligence (AI) in electoral processes is a crucial area of focus for Ukraine, especially considering its ongoing efforts to align with European Union acquis amidst a full-scale war and challenging external situation. This paper explores the intersection of EU AI Act risk-based approach and its future implementation by Ukraine, highlighting both the opportunities and risks associated with the implementation of the EU AI regulation in the context of Ukrainian electoral processes.

The paper outlines the definitions and context of AI, emphasizing its potential to both enhance and disrupt electoral integrity. It explains the technical and perceptual dimensions of AI's impact on elections, including applications in pre-electoral, electoral, and post-electoral periods. The role of AI in both augmenting governmental efficiency and posing significant risks through manipulation and misinformation is critically examined through the newly established EU AI act. This document delves into the current regulatory framework for AI within the EU, particularly focusing on the AI Act and its implications for member states and candidate countries like Ukraine. The AI Act's risk-based approach to regulating AI technologies, including high-risk applications relevant to electoral processes, is detailed. The paper also covers the governance structure supporting the AI Act, including the establishment of the AI Office and the roles of various EU bodies in ensuring compliance and oversight.

By applying technical and perceptual approaches to leveraging AI technology, pre-defining challenges and opportunities in governance across it, this paper presents a set of recommendations for Ukrainian policymakers, government, Central Election Commission of Ukraine, and civil society, grouped into short-, medium-, and long-term actions. These recommendations aim to strengthen institutional capacities, enhance collaboration between public and private sectors, ensure robust accountability mechanisms in future legislation, and build comprehensive capacity and training programs. The goal is to provide a clear pathway for Ukraine to effectively integrate and regulate AI in its electoral processes, ensuring transparency, accountability, and alignment with EU standards.

Adapting EU Artificial Intelligence Regulations for Electoral Processes: A Path for Ukraine

Lead authors:
Andrea Castagna, Anna Melenchuk

Co-authors:
Igor Tkachenko, Oleksii Sydorchuk

Reviewers:
Lisa Reppell, Ingrid Bicu

This policy paper was developed by the Institute of Innovative Governance (IIG) in cooperation with the International Foundation for Electoral Systems (IFES) with the support of the United States Agency for International Development (USAID) and UK aid. The opinions expressed herein are those of the authors and do not necessarily reflect the views of USAID, the United States Government or the UK government.

USAID FROM THE AMERICAN PEOPLE

UKaid from the British people

International Foundation for Electoral Systems IFES

Institute of Innovative Governance

Acknowledgements

We express our gratitude to the individuals who contributed insights and feedback on the subject matter of this report:

- Serhii Postivyi – Member of the Central Election Commission of Ukraine
- Anna Bulakh – Head of AI Ethics and Partnerships at Respeecher
- Oleh Dubno – Legal Consultant on AI at the Ministry of Digital Transformation
- Max Dvorovyi – Legal Expert at the Digital Security Laboratory
- Maksym Tereshchenko – Co-Founder at Urban Space 500
- Olga Guzhva – Head of Cybersecurity at Internews Ukraine
- Anna Mysyshyn – Director at the Institute of Innovative Governance

About IFES Ukraine

In Ukraine, IFES efforts to strengthen democratic progress are supported by the United States Agency for International Development, Global Affairs Canada, and UK aid. To date, these efforts have led to unprecedented progress in:

- ensuring free, fair, and inclusive elections;
- advancing political integrity;
- strengthening Ukraine's digital transformation and cybersecurity resilience;
- championing the political and electoral rights of all Ukrainians;
- fostering informed and engaged citizenship.

Table of Contents

Introduction

Definitions and context

In the rapidly evolving landscape of modern governance, the intersection of Artificial Intelligence (AI) and electoral processes stands as a crucial juncture, necessitating a clear understanding of both concepts for informed discourse and decision-making. This is particularly true for Ukraine, a country that is facing unprecedented Russian full-scale aggression while implementing some crucial reforms for its democratic and security consolidation. As artificial intelligence (AI) and its potential influence on elections gain prominence, not only electoral management bodies (EMBs) but also policymakers, government, civil society, and international organizations must develop strategies to address and, when appropriate, leverage AI to ensure post-war elections in Ukraine are free, fair, and secure. As a rapidly advancing set of technologies, AI is largely unregulated, and there has been limited research on its potential effects on the electoral process. Thus, collaborative efforts are essential to understand and mitigate AI's risks, enhance electoral integrity, and build robust frameworks that safeguard democratic principles in the evolving digital landscape.

Artificial Intelligence or AI (also known as Algorithmic Intelligence) is an umbrella term that encompasses a wide variety of technologies. According to the Massachusetts Institute of Technology (MIT), AI is defined[1] as the ability for computers to imitate cognitive human functions such as learning and problem-solving. Another more policy-oriented definition has been provided by the High-Level Expert Group on Artificial Intelligence set up by the European Commission in 2019 which has defined AI as "systems that exhibit intelligent behavior through the analysis of their environment and the execution of actions – with varying degrees of autonomy – to accomplish specific goals." Moreover, AI can be integrated[2] into hardware devices (e.g., sophisticated robots, autonomous vehicles, drones, or Internet of Things applications) and interact outside the virtual sphere.

The imitation of cognitive functions is often possible through machine learning (ML) that is defined[3] as the capacity of human-made technologies to extract patterns from collected data and apply them to new tasks that they may not have completed before. In other words, through patterns extracted through ML, modern AI can often simulate the reasoning that people use to learn from new information, make decisions and produce outputs. While discussing the technical implications of the relationship between AI and ML falls beyond the scope of this report, the practicalities of such relationship are, on the contrary, extremely significant. In this regard, a particular area of interest lies within the e-government sector and other associated domains, such as e-voting (or electronic voting, which includes a broad spectrum of technologies like electronic machine voting, internet voting, etc.). Indeed, e-voting can be broadly defined[4] as a method of voting that utilizes electronic technology to assist or manage the process of casting and counting ballots. For the scope of this paper, e-voting falls within the broader realm of e-government. E-government (or electronic government) is defined[5] as the utilization of ICTs to deliver government services to citizens and businesses with improved effectiveness and efficiency.

Within the e-government sphere, various nomenclatures have been developed to categorize distinct and complementary types of digital governance initiatives, each serving specific purposes and stakeholders.

1 Artificial Intelligence vs Machine Learning: What's the difference? https://professionalprograms.mit.edu/blog/technology/machine-learning-vs-artificial-intelligence/

2 A definition of Artificial Intelligence: main capabilities and scientific disciplines. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

3 What is machine learning (ML)? https://www.ibm.com/topics/machine-learning

4 Electronic voting. https://www.britannica.com/topic/electronic-voting

5 eGovernment and digital public services. https://digital-strategy.ec.europa.eu/en/policies/egovernment

Such classifications[6] include:

- Government-to-Government (G2G), which emphasizes data sharing and electronic exchanges among governmental bodies at various administrative levels,
- Government-to-Business (G2B), focusing on facilitating business-specific transactions and services tailored to commercial entities, and lastly,
- Government-to-Citizen (G2C) initiatives prioritize enhancing citizen engagement and interaction with government services, encompassing activities related to public service delivery and creation of tools that allow the citizen participation in decision-making processes. The creation, implementation, and management of technologies such as electronic voting, participatory budgeting, and internet voting are classified as G2C.

At the same time, the active participation of citizens through e-voting systems (for instance, during elections), the use of participatory e-voting platforms (for example, through participatory budgeting tools) and any other active engagement of citizens participation in a decision-making system through ICT tools is classified as Citizens-to-Government (C2G).

In recent years, the above-mentioned technologies, which are widely used for election processes for such purposes as analysis of voter authentication, voter lists maintenance, campaign finance analysis, voter education and awareness, fraud prevention, cybersecurity, and e-voting, have become increasingly associated with the development of AI. From streamlined service delivery to enhanced accessibility and responsiveness, the integration of AI into G2C and C2G initiatives has the potential to revolutionize the way citizens interact with their governments (and vice versa) during elections. In particular, two main areas are affected by this change: the technical and perceptual dimensions.

Technical dimension: By technical dimension, we mean that AI and ML are altering the landscape of e-voting technologies, both those designed to be overseen by election officials and those intended for remote e-voting. For example, systems of e-voting and e-government are expected[7] to be significantly influenced by the integration of AI technologies. This is an area whose full impact is perhaps yet to be experienced and analyzed but concrete examples. For instance, AI-driven solutions can enhance the accessibility of e-government solutions, by providing alternative voting methods, such as voice recognition or text-to-speech interfaces that can ensure a higher participation of voters. In addition, in the next few years, AI is expected to bolster the security measures of e-voting systems and e-government systems by detecting and mitigating potential threats, analyzing patterns of behavior to identify anomalies, and flagging suspicious activities in real-time, thus safeguarding the integrity of election. Last but not least, AI-powered data analytics is expected to provide government agencies with insights derived from large datasets related to electoral participation and trends in the usage of e-voting and e-government tools. In addition to these examples, one can expect the development of technical aspects of e-voting and e-platforms as well. For example, in the future, AI algorithms can be used to identify and exploit vulnerabilities in system architecture, launch sophisticated phishing attacks, or conduct large-scale distributed denial-of-service (DDoS) attacks to disrupt e-government services or manipulate election outcomes within e-voting platforms.

Perceptual Dimension: On the other hand, we have already seen that AI and ML have played an important role in the so-called perceptual dimension of elections or, in other words, how voters see and perceive the electoral process as such. For instance, deep fakes and other generative AI disinformation tools have already influenced how elections are perceived by citizens. AI technologies can be used to generate and disseminate false information or propaganda, which can influence voter opinions or undermine trust in government institutions. By analyzing large datasets, AI algorithms can identify vulnerable populations

6 Four Kinds of E-Governance: A Stakeholder Analysis. https://www.gdrc.org/u-gov/egov-03.html

7 Artificial Intelligence in the public sector. https://joinup.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/artificial-intelligence-public-sector

and tailor disinformation campaigns to discourage them from participating in elections or engaging with government services.

The scope of the paper, as highlighted in the next paragraph, is therefore focused on examining how the technical and perceptual dimensions of citizens' interaction with elections are influenced, using Ukraine as a case study to explore and provide concrete and specific recommendations. These recommendations are tailored to the specific context of Ukraine but are also intended to serve as general guidance on strengthening electoral integrity in an era of rapid AI and ML adoption.

Purpose, overview, and target audience

This policy paper (drafted in August 2024) has been developed by experts from the Institute of Innovative Governance (IIG) in cooperation with the International Foundation for Electoral Systems (IFES) Ukraine. It has been designed with a multifaceted approach, aiming to provide policy support in order to identify risks and opportunities of using AI in future Ukrainian elections. Consequently, the paper offers clear and precise policy recommendations aimed at supporting Ukrainian integration into European Union, particularly in domains related to artificial intelligence and electoral processes. We explore how this alignment will impact democratic procedures within Ukraine and foster greater compatibility with EU standards in emerging technology that are relevant for electoral processes. Our policy recommendations will be designed to facilitate alignment with EU standards and promote the harmonization of AI legislation, ultimately bolstering Ukraine's progress towards European integration. By providing such recommendations, the aim is to ensure that Ukrainian policymakers and stakeholders have additional instruments to align with EU AI regulations.

In particular, two macro-dimensions will be analyzed in this paper: the technical and the perceptual dimension. On the one hand, we explore the relation of AI and other technical aspects of electoral technologies (such as e-voting and e-government). At the same time, this paper analyses other risks associated with AI in the context of electoral processes such as disinformation and manipulation of public opinion through AI generated contents. Ultimately, our purpose is to offer a precise and current depiction of Ukraine's status quo regarding the adaptation of EU's artificial intelligence regulations for electoral processes and provide recommendations for a broad range of stakeholders involved in the area of AI and elections in Ukraine in the context of European integration of Ukraine.

One of the core aspects of this investigation is the process of European integration in the AI sphere. Since February 2022, Ukraine has been subject to a full-scale aggression from the Russian Federation, with the aim of destabilizing and dismantling Ukraine as an independent and democratic nation. For this reason, Ukrainian society, including its government institutions, public bodies, civil society organizations, and individual citizens, has mobilized unparalleled resources to fight this external threat to its sovereignty and democratic institutions. At the same time, on June 23, 2023, the European Council granted Ukraine the status of a candidate for accession to the European Union (EU) and, few months later, the European Commission recommended opening accession negotiations with Ukraine. This implies that Ukraine will encounter an unprecedented situation, one that has no parallel in the modern European history. On one hand, Ukraine will need to continue in its fight against full-scale Russian aggression. On the other hand, Ukraine has pledged to adopt the comprehensive collection of common legislation and obligations that make up the body of EU law, known as the EU Acquis. This commitment entails an unprecedented level of reform, democratic scrutiny, and policy negotiations.

This process is particularly relevant in the context of this paper as it will have strong implication of the adoption of AI regulation. Hence, in this report, the scope is to offer a short yet comprehensive description of how the EU has regulated AI, detailing both the methods employed and the extent of regulation implemented, and the risk-based approach that has direct and relevant implication for electoral processes in Europe and beyond. We aim to furnish readers with a thorough understanding of this landmark legislation and its ramifications for electoral procedures, with a particular focus on the technical and perceptual dimensions.

The target audience of this position paper comprises Ukrainian and EU policymakers interested in the areas of emerging technologies (such as AI and ML), as well as those who are interested in democratic consolidation, electoral processes, and electoral integrity in Ukraine. Through the policy recommendations, the objective is to furnish policymakers and stakeholders with concrete suggestions and guidance for enhancing AI policy in Ukraine and electoral integrity. Additionally, the paper caters to scholars and researchers with a particular interest in understanding the specific challenges Ukraine is currently facing with.

EU Standards & Regulatory Framework

This chapter introduces the AI Act, focusing on its status as EU regulation, its impact on EU member states, and its compatibility with other important EU legislation. It is often under-reported that the EU only possesses the competences (powers) granted to it by the treaties (principle of conferral). According to this principle, the EU can only act within the boundaries of the competences granted to it by the member states in the treaties. Moreover, competences not delegated to the EU in the treaties remain under the authority of the member states. Such principle of subsidiarity applies not only to current EU member states but also (to a certain extent) to countries aspiring to join the EU, such as Ukraine. The EU accession process entails meeting the accession criteria, which include the adoption and implementation of the European acquis. In practical terms, the acquis is the accumulated legislation, legal acts, and court decisions that constitute the body of European Union law. The so-called acquis chapters (currently 35) serve[8] as the foundation for the accession negotiations with each candidate country.

These chapters represent various aspects of the acquis that require reforms for meeting the conditions of accession. Candidate countries must adjust their administrative and institutional infrastructures and align their national legislation with EU laws in these areas. Moreover, the chapters undergo review during the screening of the acquis and are regularly evaluated until each chapter is concluded.

When it comes to a broad legislative topic such as artificial intelligence, the number of competences and relevant topics that pertain to acquis chapters is extremely broad. For instance, they range from European harmonized rules for the placing on the market to measures to support innovation and SMEs. Therefore, it is not surprising that in the last few years, the EU has placed a very strong emphasis on creating a comprehensive legislative text that consolidates all these elements into a single piece of legislation: the AI Act. And Ukraine, as an EU candidate country, is expected to incorporate in the upcoming years the AI Act into its own national legislation as part of the process of accession into the European Union. Therefore, understanding of the AI Act is extremely important to fully understand the impact of AI in future electoral process in Ukraine. In particular, the EU AI Act serves as a comprehensive framework, potentially influencing a broad spectrum of fundamental rights issues, such as the right to vote as stated in Article 39 of the Charter of Fundamental Rights of the European Union which is mentioned in the AI Act preamble. The AI Act aims to ensure fundamental rights, democracy, and the rule of law. Its Recital 48 specifies criteria for identifying high-risk AI systems, which include the potential to harm fundamental rights, such as the right to vote[9].

The EU AI Act and the AI Office

The AI Act was initially proposed by the European Commission in April 2021 and is considered as the first comprehensive regulation on AI in the world. In EU legislative terms, it is a regulation, which means it is a legal act that applies automatically and uniformly to all EU countries upon entry into force, without the need for transposition into national law of the member states. In other words, it is binding for all EU member states and national authority's member states need to ensure that it is fully in force. This means that, after the transition period (set to 24 months by the AI Act), all 27 EU member states should have created the practical conditions

8 Chapters of the acquis. https://neighbourhood-enlargement.ec.europa.eu/enlargement-policy/conditions-membership/chapters-acquis_en

9 For further details, see "Is election integrity integral to the Artificial Intelligence Act?" available at: https://epd.eu/content/uploads/2024/07/Is-election-integrity-integral-to-the-Artificial-Intelligence-Act_-1-1-7.pdf.

to ensure its full implementation[10], including establishing rights and obligations for individuals and enabling them to invoke it directly before national courts.

The AI Act's discussion and approval process has been quite complex and involved many discussions and meetings between EU policy makers from the European Council, the European Parliament, the European Commission, member states bodies, and a large number of European and international stakeholders.

The final form of this new EU act, approved in March 2024, establishes obligations for AI based on its potential risks and level of impact in multiple areas, including in the area of electoral competition. Essentially, the AI Act functions as consumer safety legislation, adopting a "risk-based approach" concerning products or services using artificial intelligence tools and features. Hence, AI applications will undergo varying degrees of scrutiny based on their level of risk associated. The AI Act is set to take effect 20 days following its publication in the Official Journal of the EU. Most of the Act's provisions will be enforceable two years after it comes into effect. However, regulations concerning prohibited AI systems will become applicable after six months, and those concerning generative AI will be enforced after 12 months. The rules for high-risk AI systems will take effect[11] in three years.

In terms of governance, the EU is currently creating a system to oversee the implementation of the AI Act and monitor advancements in AI within the EU member states. The main component of this governance system[12] is the AI Office, a centralized office which will sit within the Directorate-General for Communication Networks, Content and Technology (DG CNECT) in the European Commission. The goal of the office will be to set standards, test new methods, and ensure that companies and bodies follow the same rules before operating within the European market. Moreover, the AI Office will be supported by advisory bodies as well. At an institutional level, the AI Office will cooperate with key stakeholders, such as the European Artificial Intelligence Board and the European Centre for Algorithmic Transparency.

Additionally, partnerships with individual experts and organizations, both within and outside EU member states, will be facilitated by the AI Office. For instance, a scientific panel of independent experts (currently being formed as of April 2024) will advise the AI Office on General Purpose Artificial Intelligence (GPAI) models and emerging high-impact AI technologies and will contribute to the development of methodologies for evaluating the capabilities of foundation models. Moreover, an AI Board, comprised of nominated representatives from EU member states, will act as a coordination platform and advisory body to both the European Commission and the AI Office, while also contributing to the implementation of the AI Act (e.g., designing codes of practice).

The AI Office will act as the Secretariat of the AI Board and intergovernmental forum for coordination between the national regulators. Also, AI Board will assist the AI Office in supporting national competent authorities in the establishment and development of regulatory sandboxes and facilitate cooperation and information sharing among regulatory sandboxes.

It is important to note that the AI Act has established precise definitions for the various actors engaged in AI, including providers, deployers, importers, distributors, and product manufacturers. This implies that all parties engaged in the development, utilization, importation, distribution, or manufacturing of AI systems will be subject to accountability measures.

Furthermore, the AI Act extends its jurisdiction to cover providers and deployers of AI systems situated outside of the EU, such as those in Ukraine, if the output or the code is generated by the system is intended

10 The EU Artificial Intelligence Act. Article 113: Entry into Force and Application. https://artificialintelligenceact.eu/article/113/

11 AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

12 The AI Office: What is it, and how does it work? https://artificialintelligenceact.eu/the-ai-office-summary/

for use within the EU. In practical terms, a provider or a distributor must ensure[13] that their AI practices adhere to transparency and practical regulatory standards. Depending on the future provisions set by the AI Office, they must conduct thorough risk assessments, utilize high-quality data, document their technical and ethical decisions, maintain records of their system's performance, inform users about the nature and purpose of their systems, facilitate human oversight and intervention, and ensure accuracy, robustness, and cybersecurity measures. Additionally, they are required to test their systems for compliance with the regulations before introducing them to the market or implementing them and register their systems in an EU database accessible to the public. This process will also be established by the AI Office.

As of today, the governance structure is still being formed, which means that members states and the EU are still in the process[14] of creating the conditions to apply the risks categories and ensure the correct monitoring of the legislation. Nevertheless, there are some considerations that can be made.

First, the AI Office is expected to contribute to the coherent application of the AI Act across the member states, including the establishment of advisory bodies at the EU level, facilitating support and information exchange, and developing tools, methodologies, and benchmarks for evaluating capabilities. This means that every risk related to AI in the field of elections will be highlighted by the AI Office itself, which will be a major stakeholder in this regard.

Second, as the European AI Board will be formed by representatives of the member states, it will act[15] as a major point of contact when it comes to reporting on the influence of the AI Act during electoral procedures. In other words, any significant events involving AI technologies that impact elections within the EU will be reported by and discussed in the AI Board.

Last, The AI Office will actively seek partnerships with individual experts and organizations, fostering collaboration among providers of AI models and systems, including those specializing in general-purpose AI, as well as with the open-source community. Through the establishment of forums for cooperation, organizations working at the intersection of AI and elections will have the opportunity to directly engage with the AI Office. This proactive engagement opens the door to various opportunities that may emerge in the upcoming months.

AI Act: Risks categories and implications for the electoral process

The level of risk posed by artificial intelligence is the practical basis of the AI Act. The regulatory framework defines four levels of risk[16] associated with artificial intelligence: unacceptable risk, high risk, limited risk, and minimal or no risk.

- **Unacceptable Risks in AI-Technologies:** For unacceptable risk, the AI Act defines all artificial intelligence systems considered a clear threat to security and people's rights. Those systems will be prohibited and won't be able to be used or activated in Europe. Examples of such systems include those that manipulate people's behaviour, like voice-activated toys that encourage children to behave dangerously or systems that classify individuals based on their behavior, socioeconomic status, or personal traits (e.g., social scoring). However, there may be exceptions for law enforcement purposes. "Real-time" remote biometric identification systems will be permitted in a limited number of serious cases, while "post" remote biometric identification systems, which identify individuals after

13 The EU AI Act: What it means for your business. https://www.ey.com/en_ch/forensic-integrity-services/the-eu-ai-act-what-it-means-for-your-business

14 MEPs approve world's first comprehensive AI law. https://www.bbc.com/news/technology-68546450

15 The EU Artificial Intelligence Act. Section 1: Governance at Union Level. https://artificialintelligenceact.eu/section/7-1/

16 The EU Artificial Intelligence Act. Section 1: Classification of AI Systems as High-Risk. https://artificialintelligenceact.eu/section/3-1/

a significant delay, may be allowed for prosecuting serious crimes but only with court approval. In the field of elections, we can anticipate that AI systems which classify individuals based on their voting behavior or deliberately spread false and manipulative information about election outcomes to vulnerable populations could be considered as falling into this category.

- **High-Risks AI-Technologies:** A second category included in the AI Act are the high-risks technologies. AI systems identified as High Risk include technology used in critical infrastructures (such as transportation or telecommunications), which could endanger the lives and health of citizens, education or professional training, or other factors that can determine access to education and career path in life (such as exam scores). AI systems at high risk will be subject to rigorous obligations before they can be placed on the market, such as risk assessment and mitigation systems. In some cases, companies will be required to record activities to ensure traceability of results produced with artificial intelligence. For example, all remote biometric identification systems are considered high risk and subject to strict requirements. In principle, the use of remote biometric identification in publicly accessible spaces is prohibited[17] and, where necessary, will be subject to very strict restrictions. It is important to note that within the AI Act, all systems used to influence the outcome of elections and voter behavior are always classified as high-risk. In particular, the final text of the AI Act remarked that AI technologies "*used to influence the outcome of an election or referendum or the voting behavior of natural persons in the exercise of their vote in elections or referenda should be classified as high-risk AI systems with the exception of AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistical point of view*" (art.40). Hence, the provisions of the AI Act are quite stringent for technologies related to elections and require several lists of provisions to ensure transparency. Such provisions have at least two major practical implications. First, it means that platforms and other systems utilizing AI in the elections field will be obliged to implement strong informative and transparency measures and take extra precautions to ensure the proper respect of the new European legislation, unless they are used for mere practical organizational tasks. For instance, it is likely that high-risk AI systems in the field of elections will be required by both European and national regulators to develop a risk management system and make it explicit to regulators. This system should consist of a continuous and iterative process throughout their entire AI technology lifecycle (art. 42a). These measures will also be complemented by strong data governance obligations. AI companies will need to ensure that testing datasets are relevant, sufficiently representative, and free of bias. In addition, regulations related to human oversight of the model and data may also be asked to be implemented by regulatory bodies. Moreover, high-risk AI technologies can be asked to provide appropriate information in the form of instructions for use, which should include the characteristics, capabilities, and limitations of the AI system operating in a specific field (such as elections) (art. 47).

- **Low and No-Risks Technologies:** Lastly, the AI Act also acknowledges low-risk and no-risk applications, which carry minimal transparency and informative obligations to ensure users are aware of their interaction with AI. AI systems with low risk, like chatbots and AI that generate images, audio, and videos, are subject to transparency requirements. These systems must inform users that they are interacting with an AI and allow users to choose whether to keep using it. Generative AI models, such as ChatGPT, must also be created and trained to avoid creating illegal content. Additionally, the creators of these AI models must provide summaries of any copyrighted data used for training. On the contrary, AI systems with no risks have minimal transparency regulations, such as disclaimers. While the AI Act doesn't explicitly state it, one can reasonably argue that these low-risk and no-risk applications have limited or no implications for elections and electoral processes. Hence, we anticipate the AI Office will not prioritize them when operating in the area of elections.

17 The EU Artificial Intelligence Act. Article 5: Prohibited AI Practices. https://artificialintelligenceact.eu/article/5/

The AI Act enumerates several penalties within its text, which constitute an integral part of the legislation. While applying fines and penalties, the AI Act outlines criteria to ensure proportional and fair enforcement. When determining whether to impose an administrative fine and its amount, all relevant circumstances of the specific situation are considered. Key factors include the nature, gravity, and duration of the infringement, the consequences, and the number of affected individuals and their level of damage. Additionally, whether other authorities have already fined the operator for the same or related infringements is taken into account. The operator's size, annual turnover, and market share are also relevant, as are any financial benefits gained or losses avoided from the infringement. The level of cooperation with authorities to remedy the infringement, the degree of responsibility and preventive measures taken by the operator, the manner in which authorities became aware of the infringement, whether the infringement was intentional or negligent, and any actions taken to mitigate harm are all crucial considerations.

Penalties for non-compliance:

- Non-compliance with the prohibition of the AI practices shall be subject to administrative fines of up to €35,000,000 or, if the offender is an undertaking, up to 7 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.
- Non-compliance with any of the provisions related to operators or notified bodies can result in administrative fines of up to €15,000,000 or, if the offender is undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year.
- The supply of incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply to a request shall be subject to administrative fines of up to €7,500,000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year.
- **Territoriality**: Sanctions apply[18] to non-compliant providers who place on the market or put into service AI systems in the EU, regardless of whether those providers are established or located within the EU or in a third country. Which basically means that, in theory, non-compliant providers that use AI technologies to influence or manipulate elections are expected to be sanctioned if they do not adhere to the transparency of the above-mentioned accountability principle.
- Moreover, the AI Act contains rules on the imposing of administrative sanctions on Union institutions, bodies, offices, and agencies falling within the scope of its provisions. The regulatory body in those cases will be the European Data Protection Supervisor. Those penalties are applied in following cases: non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to €1,500,000.
- Non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5, shall be subject to administrative fines of up to €750,000.

Challenges in the AI and elections: Disinformation within EU and beyond

Currently, one of the primary challenges concerning AI and elections is disinformation and manipulation of information, which presents a significant threat for electoral procedures (perceptual dimension). For example, generative AI can be exploited to manipulate content related to information about elections thereby influencing electoral behavior and trends. For example, an example of this threat is the exploitation of Generative AI which can potentially open the door to disinformation and manipulation of electoral content. As technological limitations are rapidly overcome by different forms of AI converge, AI's persuasive potential may increase

18 The EU Artificial Intelligence Act. Chapter XII: Penalties. https://artificialintelligenceact.eu/chapter/12/

over time and some AI systems could enable manipulation that take the form of fake news, deepfake videos, or AI-generated social media posts designed to deceive users.

While the AI Act does not directly link high-risk technologies that influence elections through disinformation, the two elements are closely interconnected within the Act itself. Disinformation and development of misleading content is one of the major issues that the AI act acknowledges throughout its entire text. In particular, the AI Act recognizes the risks of disinformation in its part related to foundation models, machine learning or deep learning models trained on extensive datasets, enabling their application across diverse use cases. The rapid pace of technological advancement and emergence of systems such as Chat GPT has prompted EU policymakers to prioritize foundation models. Generative AI systems constitute[19] a specific subset of foundation models, specifically intended to autonomously generate content such as complex text, images, audio, or video, with varying degrees of autonomy.

It is important to note that in the AI sector, representing technological realities through mere legal definitions appears particularly challenging and difficult from a regulator perspective. For instance, the so called "Generic GPAI models" are subject to mere transparency obligations[20], consisting of guaranteeing the availability of technical documentation that makes their functioning understandable.

On the contrary, "Systemic GPAI models" (which the AI Act text recognizes as those that pose a systemic risk to the European Union in terms of public security, fundamental rights, or society as a whole, and that can be propagated at scale across the value chain) are subject to the same obligations as basic GPAI models, plus a more pervasive regulation and set of obligations. These include[21] carrying out the evaluation of the model in accordance with standardized protocols (elaborated by the European Commission) and tools that reflect the state of the art, including the conduct and documentation of 'adversarial tests' in order to identify and mitigate systemic risk.

We can therefore expect that, in accordance with the AI Act, a provider of a foundation model that operates in the field of election must demonstrate, before releasing their model to the market, how they have addressed foreseeable risks to public safety, fundamental rights, democracy, and the rule of law. This includes designing, developing, and testing the foundation model to ensure performance, predictability, interpretability, corrigibility, safety, and cybersecurity throughout its lifecycle.

Also, significant concern arises from Systemic GPAI models spreading disinformation in social media platforms. AI-driven microtargeting techniques employed in political campaigns can manipulate and tailor messages to specific demographic groups, potentially influencing their opinions and voting behavior. This may contribute to the fragmentation of the electorate, as individuals receive tailored messages that reinforce their biases and preferences, rather than promoting informed and balanced discourse during electoral campaigns. Several recent notable examples are presented below:

- A few days before Slovakia's 2023 parliamentary elections, deepfake audio recordings surfaced, falsely portraying Michal Šimečka, leader of the Progressive Slovakia party and pro-western politician, discussing election manipulation. Spread across social media platforms, the deepfake aimed to sway public opinion and influence the outcome of the election. Although Šimečka denounced the audio as fake and reported the disinformation through the EU's DSA (see next paragraph), the deepfake continued to circulate widely. Researchers in Slovakia speculated[22] that the vote-rigging deepfake was the work of the Russian government, though no conclusive evidence has been provided yet.

19 The EU Artificial Intelligence Act. Chapter V: General-Purpose AI Models. https://artificialintelligenceact.eu/chapter/5/

20 The EU Artificial Intelligence Act. Section 2: Obligations for Providers of General-Purpose AI Models. https://artificialintelligenceact.eu/section/5-2/

21 The EU Artificial Intelligence Act. Article 53: Obligations for Providers of General-Purpose AI Models. https://artificialintelligenceact.eu/article/53/

22 "A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning." https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html

- The most recent case occurred during the European elections campaign and was connected to the spread of misinformation by Google, Microsoft, and OpenAI chatbots. According to Democracy Reporting International, the chatbots were providing false information[23] on election date and voting procedure.
- In 2024, another case took place in France where an AI-generated deep fake video portrayed[24] young members of the election candidate's family spreading racist comments ahead of the European elections.

These cases underscore the importance of a robust AI legislative framework, such as the AI Act, in combating disinformation. However, it also highlights that disinformation remains one of the most significant challenges democratic societies will confront in the intersection of AI and elections. Despite regulatory efforts, the rapid evolution of AI technology and the proliferation of sophisticated disinformation tactics pose ongoing threats to the integrity of democratic processes.

Other examples of EU standards in the field

While the AI Act helps to establish a robust regulatory framework in artificial intelligence, other EU laws, such as Digital Service Act (DSA) and Digital Market Act (DMA), also have important implications for elections, particular, in terms of electoral integrity. DSA and DMA were drafted in times when the AI discussions were just taking shape, therefore, while being relevant for AI regulation landscape, they do not include any specific measures related to the use AI. However, these Acts are relevant to the responsibilities of the AI Office, as described in the sub-section 2a of this paper, especially for coordinating oversight of AI systems governed by the AI Act. Understanding the interplay between these regulations is crucial for a holistic approach to managing AI's impact on electoral integrity.

The Digital Service Act (DSA)

The DSA is a regulation of the EU that entered into force on August 25, 2023. Its launch marks a significant step in regulating very large online platforms (VLOPs) and very large online search engines (VLOSEs). Indeed, the DSA imposes[25] specific obligations on online platforms to combat the sale of illicit goods and services, addresses the dissemination of illegal content while upholding fundamental rights, and sets limits on advertising presentation. These prescriptions obviously have direct implications for elections as well.

For example, under the DSA the European Commission has issued guidelines to mitigate systemic online risks affecting election integrity, particularly focusing on the upcoming European Parliament elections in June 2024. Under the DSA guidelines, services with over 45 million active users in the EU are mandated to mitigate risks related to electoral processes while preserving fundamental rights, including freedom of expression. These guidelines advocate for the promotion of official electoral information, implementation of media literacy initiatives, and adjustments to recommender systems to curb the monetization and virality of disinformation that can potentially influence voting results. Although the guidelines lack direct implications for AI regulations, they bear significant weight in combating disinformation potentially generated with AI.

23 "AI chatbots spread falsehoods about the EU election, report finds." https://www.politico.eu/article/ai-chatbots-spread-falsehoods-about-the-eu-elections-report-finds/

24 "Viral deepfake videos of Le Pen family reminder that content moderation is still not up to par ahead of EU elections." https://www.euractiv.com/section/artificial-intelligence/news/viral-deepfake-videos-of-le-pen-family-reminder-that-content-moderation-is-still-not-up-to-par-ahead-of-eu-elections/

25 The Digital Services Act package. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

The Digital Market Act (DMA)

The DMA is a regulation of the EU that was approved in 2022 and aims to regulate Europe's digital market. DMA establishes a stringent set of objective criteria for identifying large online platforms as "gatekeepers" or platforms that due to their size, and number of users have a dominant market position such as Google, Facebook, Amazon etc. Gatekeepers' criteria encompass[26] factors such as the company's economic position, substantial impact on the internal market across multiple EU countries, and its significant intermediation role between a large user base and numerous businesses.

DMA has been fully enforced in 2024 following nearly two years of transition and users to choose the services they wish to utilize (or not). However, it also holds implications for electoral processes, for example by requiring gatekeepers to obtain explicit user consent for tracking online behavior for advertising purposes, thus enhancing transparency in political advertising.

26 The Digital Markets Act: ensuring fair and open digital markets. https://Registered Parties | Parties and Foundations | Authority for European Political Parties and
European Political Foundations (europa.eu)

The Status Quo in Ukraine

Having explored the concepts and AI-related regulatory frameworks in the EU in the previous chapter, this chapter focuses specifically on the case of Ukraine, an EU candidate state that faces unprecedented wartime challenges related to the adaptation of the EU regulations, including in the area of elections, amidst the Russian full-scale invasion.

The current political context in Ukraine amidst the Russian full-scale aggression

According to Ukraine's Constitution, parliamentary elections cannot be held until martial law is lifted with a subsequent six-month period mandated. The Ukrainian President Volodymyr Zelenskyy declared martial law on 24 February 2022, in response to the Russian full-scale invasion. Since then, the martial law has been extended several times, with the last declared extension in May 2024 (as of time of drafting this paper), in line with the Ukrainian Constitution.

Hence, as of today, it is very unlikely that presidential elections (or any other elections) will be organized in Ukraine anytime soon. Therefore, it is unlikely that Ukraine will be able to test and implement AI features in elections during the war. Moreover, it is also highly improbable that Ukraine will have the opportunity to explore and integrate AI functionalities into its electoral processes and any other G2C/C2G system and e-government features.

At the same time, Ukrainian civil society and start-up community are developing various initiatives or that use generative AI and natural language processing to detect, defend, and counteract disinformation which may help to protect Ukrainian voters from targeted information manipulation and eventually have a positive impact on possible future elections in Ukraine. For example, Ukrainian start-up Mantis Analytics[27] processes thousands of messages and gigabytes of data from mass media, social networks, and information platforms in real time. Then it arranges the data on an interactive map. Another Ukrainian AI-powered start-up, Osavul[28], analyzes the web environment, social networks, in particular Telegram, by measuring quantitative and qualitative indicators of potential threats, identifying the primary source, and signs of coordination among those who spread disinformation.

Therefore, this chapter looks into potential challenges related to the use of AI in elections in Ukraine. With regards to technical application of AI in elections by those who organize them, it should be noted that within the current Ukrainian context, the implementation of e-voting platforms (even without AI features) and remote voting for elections poses several unresolved issues. Firstly, martial law prohibits Ukrainian authorities from conducting elections, thus hindering the proper testing and implementation of AI tools and other technical features for a pilot phase in local elections (such as local referenda and e-voting/remote voting at the local level). Secondly, the full-scale Russian invasion presents unprecedented challenges in terms of cybersecurity, cyber defense, and information security, potentially jeopardizing the implementation of new AI systems. Finally, the Ukrainian government has prioritized other areas when it comes to AI, as outlined in the next chapter.

27 Mantis Analytics. Protect Cognitive Security in Real-Time. https://mantisanalytics.com/

28 Osavul - an AI-powered security against information threats. https://www.osavul.cloud/

AI regulation in Ukraine

While Ukraine is not foreseen to implement any AI integrations neither for general purposes, nor in its electoral process, the level of interest by the government and its citizens remain quite high and AI policy discussion take place in various fields. While one can argue that Ukraine is still at an early stage of AI regulation, particularly when compared with the EU, Ukrainian authorities have achieved a few important results.

The AI regulatory landscape in Ukraine involves representatives of the government, parliament, private sector, and educational and scientific institutions. While the detailed institutional framework and responsibilities on regulating AI is expected to be defined with the transposition of the AI Act into Ukrainian legislation as a part of EU acquis, a few key institutions and organizations play a prominent role in today's AI landscape in Ukraine.

First and foremost, the Ministry of Digital Transformation is the main executive body responsible for development, coordination, and implementation of the public policy in the sphere if AI. In particular, the Ministry plays a crucial role in ensuring the development of AI (according to the 2019 Regulation of the Cabinet of Ministers of Ukraine "On the Ministry of Digital Transformation"[29]).

Expert Committee on the Development of Artificial Intelligence in Ukraine[30] was established under the Ministry of Digital Transformation in 2019. Its primary objective is to devise policy and practical strategies aimed at enhancing Ukraine's competitiveness in the area of AI. Functionally, the Committee operates across four distinct yet interconnected workstreams: AI in Public Administration, AI in Education, AI in Security/Defense, and AI Regulation.

The first milestone achieved was the publication of the 2020 Concept of AI development in Ukraine[31] and 2023 AI roadmap for Ukraine[32]. Indeed, the Expert Committee and Ukraine's Ministry of Digital Transformation released a detailed plan[33] for regulating AI and fostering innovation in the field through two primary processes: supporting local businesses in Ukraine in preparing for AI regulatory laws, such as the EU's AI Act, and educating people on managing AI-related risks.

Moreover, the AI regulation roadmap is built upon a few key principles. First and most importantly, it is the principle of balance between regulation and innovation. The roadmap recognizes that Ukrainian business and citizens need time to adapt to future regulation and therefore the Ukrainian authorities want to await outcomes from comparable initiatives (such as the AI Act) and replicate good practices in the C2G/G2C and related fields. Second, a culture of self-regulation is foreseen as a possible solution before implementing stricter regulations. In other words, a collaborative approach involving the government, citizens, and businesses will be employed[34], along with the development of additional tools (such as White Papers and Recommendations) to prepare for future Ukrainian legislation and entry into the EU market. Third, the future regulations in the Ukrainian legislation will be based on a bottom-up approach and gradual progression from smaller to larger regulations and from non-legislative mechanisms for industry preparation to the enactment of the laws on AI.

An important remark to make is that, at this stage, the roadmap does not mention any specific feature or element that has a direct link with the field of elections. However, since the roadmap explicitly states that Ukraine is anticipated to adopt features of the EU AI Act and eventually incorporate the provisions outlined in this document, it can be argued that a certain level of risk categorization will be implemented in the

29 Regulation of the Cabinet of Ministers of Ukraine "On the Ministry of Digital Transformation." https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF/print

30 Expert Committee on the Development of Artificial Intelligence in Ukraine. https://ai.org.ua/

31 Regulation of the Cabinet of Ministers of Ukraine "On the Concept of AI development in Ukraine." https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

32 AI roadmap for Ukraine. https://bit.ly/3AzbW6F

33 A road map of AI regulation in Ukraine. https://ai.org.ua/a-road-map-of-ai-regulation-in-ukraine/

34 Draft Law No. 8153 "On Personal Data Protection." https://itd.rada.gov.ua/billInfo/Bills/Card/40707

future. This category is likely to resemble or mirror the high-risk category delineated by the AI Act concerning elections and therefore implement risks mitigation features to safeguard electoral processes.

Another crucial document linked to the Roadmap is the 2024 Guidelines[35] published by the Ministry of Digital Transformation on the responsible use of artificial intelligence (AI) by media companies and media professionals. The guidelines target all AI systems, regardless of whether they are developed by media entities (such as newspapers, media outlets, or large digital media companies) or by third parties. They also encompass those utilized by journalists and other media professionals, such as graphic designers and content creators.

The core of the guidelines encompasses various principles, including transparency in AI system utilization, distinct identification between human-authored and AI-generated content, prioritization of human involvement in content creation, and media self-regulation (which is very much in line with the previous mentioned roadmap).

Also, the document offers explicit guidance on what aspects media should consider when choosing AI systems for their operations, as well as methods for assessing the ethical and factual accuracy of AI-generated content. It particularly draws upon recommendations from committees within the Council of Europe and the policies of renowned global media entities in Europe and beyond. Furthermore, it furnishes detailed directives on content management and the utilization of AI across platforms, including tasks like content search and verification, translation or transcription services. Once again, while it doesn't offer clear recommendations for electoral purposes, it presents several elements that somewhat reflect the AI Act, particularly regarding technologies referred to as GPAI models in the Act. The guidelines specifically address how criteria of transparency and accountability should be applied and their potential societal risks. However, unlike the AI Act, these guidelines take a less normative and more declarative approach. In other words, they don't propose any legally binding provisions or strict recommendations but instead highlight good practices to adopt in specific circumstances. And in doing so, it fully respects the principles outlined in the above-mentioned roadmap.

In July 2024, the Ministry of Digital Transformation published the draft White Paper on AI regulation in Ukraine. This document proposes a phased approach to manage the development and implementation of AI technologies, emphasizing the protection of human rights and fostering business competitiveness. The document highlights a "bottom-up" strategy, focusing initially on non-legislative tools to prepare businesses for future regulations. It introduces mechanisms like regulatory sandboxes, impact assessment methodologies, and voluntary AI labeling to ensure compliance with future national and EU legislation. This approach aims to balance innovation with ethical considerations, addressing risks such as discrimination and misuse of AI, ensuring that human rights are protected both online and offline. The ultimate goal of the White Paper is to harmonize Ukraine's AI regulatory framework with EU standards, promoting transparency, accountability, and the responsible use of AI technologies.

Another prominent actor that is increasingly being involved in AI regulation discussions is the Committee on Digital Transformation of the Ukrainian Parliament. Together with the Ombudsperson's Office in Ukraine and the Ministry of Digital Transformation, the Committee is working on digital rights protection, including cases related to the use of AI and data protection.

Finally, Ukraine's data protection legislation that should be inherently linked with any future AI legislation needs sufficient modernization to be able to cater for AI regulations in electoral processes. This is true for the future implementation of the EU AI Act which contain provisions that enable penalties applying by the European Data Protection Supervisor to the EU institutions, bodies, offices, and agencies in cases where there is a risk of personal data or business secrets leak. Moreover, since AI applications that target voters can

35 "Ukraine: Ministry of Digitization releases AI guidelines for media." https://www.dataguidance.com/news/ukraine-ministry-digitization-releases-ai-guidelines

use personal data extensively to produce tailored messages and potentially sow disinformation, the proper legal protection of personal data is necessary. In addition, if election administration bodies use AI for voter registration and verification, the scope of personal data they can access shall also be properly outlined in the law.

The key problem of personal data protection in Ukraine is the lack of an effective national system of personal data protection in line with EU acquis and an appropriate mechanism for bringing to liability. The Draft Law No. 8153[36] on Personal Data Protection is intended to adhere Ukraine to the EU GDPR standards by creating a framework for the protection of personal data in both public and private sectors, as well as to assist bodies with the right of legislative initiative in developing regulations governing the processing of personal data and their security.

In Ukraine, the administration and oversight of elections, particularly regarding the use of technologies like AI, involve multiple entities with distinct responsibilities. The Central Election Commission (CEC) and lower-level commissions are tasked with administering the election process, which includes creating of constituencies, registering candidates, managing the voting process, tabulating votes, and establishing the election results. In parallel, the National Agency on Corruption Prevention (NACP) oversees election contestants by monitoring political finance disclosure, ensuring transparency in donations, and verifying the proper use of funds during electoral campaigns. This division of duties ensures thorough oversight and administration to maintain the integrity and transparency of elections in Ukraine. However, this split in responsibilities does not address the improper use of AI in elections.

Additionally, the National Council of Television and Radio Broadcasting of Ukraine (NCTRB) as an independent body that is not a part of executive power, plays a crucial role in overseeing online media platforms under the new Media Law, which took effect on 31 March, 2023. This law aligns Ukrainian media regulations with EU standards, particularly the EU's Audiovisual Media Services Directive. The NCTRB, in collaboration with other bodies, is responsible for defining and updating criteria for classifying online media and ensuring compliance with media laws. This includes monitoring content to prevent violations such as hate speech and propaganda. Online media can voluntarily register with the NCTRB, gaining benefits such as eligibility for public procurements, state grants, and official journalist status. The Regulator enforces content requirements and ensures platforms adhere to transparency and legal standards. However, the new law does not contain provisions detailing how to regulate the use of AI or how to detect fraud if AI-generated content affects elections. This gap highlights a critical area where additional regulatory measures are needed to address the proper or improper use of AI in the electoral context, ensuring that new technologies do not undermine the fairness and integrity of elections in Ukraine.

Last, it is important to remark that when it comes to its international positioning in the AI readiness field, the Oxford AI Readiness[37] Index has recognized Ukraine as a relatively successful country in terms of its preparation for artificial intelligence, despite the fact that the country is at war. This recognition highlights Ukraine's notable progress and proactive measures in the AI regulation landscape, including the development of the roadmap for the regulation of AI by the Ministry of Digital Transformation designed to assist Ukrainian companies to prepare for future AI regulation. Hence, the country's initiatives in creating a supportive environment for AI development highlight its preparedness to utilize AI for future growth and innovation, including in the field of elections. Challenges and opportunities related to the use of AI and elections in Ukraine.

Having outlined the current status quo in terms of AI regulations in Ukraine, this paragraph aims at outlining specific challenges and opportunities faced by Ukraine in this field. Since there are not a lot of practices of using AI in governance/elections and since post-war elections will be held in precarious security situation, there are several challenges related to use of AI in next elections.

36 Draft Law No. 8153 "On Personal Data Protection." https://itd.rada.gov.ua/billInfo/Bills/Card/40707

37 Government AI Readiness Index 2023. https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-1.pdf

This paper explores the challenges of AI in elections through technical and perceptual dimensions, utilizing the electoral cycle framework to categorize AI applications across pre-electoral, electoral, and post-electoral periods, with a comprehensive breakdown of AI uses and potential risks for each phase presented in Annex 3.

The challenges and opportunities section represents a simplified version of SWOT model which was developed with input from expert interviews conducted for the purpose of this paper.

Challenges

- **Focus on AI & security rather than AI in elections:** The current focus of the Ukrainian government and stakeholders is primarily on defense-related matters. As a result, their main efforts are directed towards the development of AI applications and technologies that can contribute to areas such as cybersecurity and defense. For example, several startups and corporate projects have emerged focusing on the utilization of AI in drone technology. Consequently, it is evident that fewer applications and technologies have been developed in other sectors, including e-government and C2G/G2C platforms. Thus, the utilization of AI for elections is not currently a policy priority for Ukraine, unless it is developed in areas related to its primary focus (security). On the other hand, there is a strong interest in supporting AI-powered solutions in the area of informational resilience and combating disinformation. Such solutions, including the ones developed by Mantis Analytics and Osavul could have a positive impact on future elections in Ukraine.

- **Level of AI familiarity not homogenous among public authorities:** Ukrainian governments have placed a strong emphasis on AI in the past, as evidenced by the Ministry of Digital Transformation's expertise in the field. However, it is also true that other public bodies, such as those involved in election organization, are much less familiar with AI development, and they do not frequently engage with AI in their daily operations. This lack of familiarity extends to AI tools, with limited knowledge about AI technologies, particularly concerning C2G/G2C platforms. Moreover, at the sub-national level, the situation is similar. At the regional and local levels, opportunities to engage with AI are quite limited, mostly through generative AI systems such as Chat GPT. Therefore, it will take time to reach the same level of understanding and familiarity with AI across all public bodies involved in elections.

- **Lack of general understanding of AI and the use of AI in elections:** Similarly, Ukrainian citizens also have limited familiarity with AI systems and the risks associated with them, particularly concerning disinformation and the use of AI in elections, such as the way AI tools might be used by candidates and parties to manipulate voters' choice. While full-scale aggression has facilitated the creation of debunking activities and practices to verify information across various segments of society, the level of understanding of the risks associated with AI, disinformation and elections remains quite low, even among educated citizens. This is not solely a problem in Ukraine, but it certainly has more consequences for Ukrainian citizens due to the prolonged Russian aggression.

- **Existing e-government tools have data privacy and cyber security issues:** In 2020, Ukraine launched Diia, a G2C system accessible through an app that enables Ukrainian citizens to utilize digital documents on their smartphones for identification and sharing purposes, eliminating the need for physical documents. The Diia portal provides access to over 130 government services. Consequently, Ukrainians are quite familiar with using apps to access public services. However, the use of the app is not yet uniform. Incorporating additional AI features into the platform related to elections and remote voting (or creating a completely different platform for it) poses cybersecurity and data privacy risks. As mentioned above, Ukraine has weak data protection and digital privacy legislation which may further aggravate any initiatives related to the use of AI in elections. Since Ukraine is not a part of the EU, the General Data Protection Regulation (GDPR) does not directly apply in its territory. Ukraine has its own non-comprehensive set of data protection legislation, which is, however, quite outdated. It needs to be reviewed in light of the new international standards and best practices. It is therefore important to align Ukrainian legislation with GDPR and other best practices before implementing AI on platforms for electoral purposes.

- **Disinformation and foreign influence:** Russia's propaganda and disinformation campaigns have accelerated with its 2022 full-scale invasion of Ukraine. Social media posts, fabricated videos and articles created by Russian troll farms are circulated in Ukraine and abroad to undermine Ukrainian government and its army. The rise of easily accessible artificial intelligence tools exacerbates vulnerabilities that Russia could exploit to undermine future elections.

- **Absence of multistakeholder coordination and debates on risks and opportunities of AI in securing Ukraine's democracy:** While Ukraine bolsters a dynamic ICT sector and strong and vibrant civil society landscape, there were only few attempts to discuss the role and impact of AI on democracy in Ukraine and develop concrete recommendations in this area. Having said that, it is important to mention that Ukraine pays attention to disinformation challenges (both foreign and internal) and some initiatives that explore the role of AI in tackling disinformation are taking place (e.g. Conference on AI and disinformation organized by the Institute of Innovative Governance in November 2023 etc.). However, that does not specifically **cover the link between AI and democracy, where elections play a fundamental role.**

- **Presence of AI gender bias:** A study[38] by the Berkeley Haas Center for Equity, Gender, and Leadership analyzed 133 AI systems across various industries and found that approximately 44 percent displayed gender bias, and 25 percent exhibited both gender and racial bias. This is a systematic problem that AI experts will need to address in the future. While this issue is not exclusive to Ukraine, its implications are particularly significant for the country, given its context as a society devastated by a war of aggression. In particular, such issues can have severe implications for the inclusivity and accessibility of AI technologies for women. Therefore, improving the understanding of AI gender bias and addressing these biases in policy forums will be imperative to ensure that AI can be effectively used in every aspect of society, including the electoral process, by everyone (including women).

38 Artificial Intelligence and gender equality. https://www.unwomen.org/en/news-stories/explainer/2024/05/artificial-intelligence-and-gender-equality

Opportunities

- **Enhance expertise in ICT and AI technology:** Ukraine possesses particular expertise and agility in the field of AI development. The above-mentioned start-ups and AI-powered initiatives that emerged during the Russian full-scale invasion to help Ukraine fight cyber threats and disinformation are clear evidence of such expertise and agility. Its ICT community, combined with educational institutions, has significant potential that could eventually position the country as a leader in the AI field. Presently, defense and cybersecurity dominate interest, but in the future, other areas, such as electoral consultation, show particular promise.

- **Improve resilience vis-à-vis fake news:** According to Ukrainian civil society experts interviewed for the purpose of this position paper, after nearly a decade of Russian aggression, Ukrainian society is better positioned than others in understanding the risks of disinformation. Ukrainians, including the older generation, are accustomed to verifying information, often through platforms like Telegram, and trusting only verified sources. This behavior stems partly from the necessity in war-torn countries to verify and debunk fake news to protect people from dangers. This tendency is less prevalent in other European states. Therefore, it can be argued that policies related to transparency and accountability for AI will be well appreciated in Ukraine and should facilitate the implementation of legislation in this particular field.

- **Commit the government to develop a flexible approach:** In the roadmap of the Ministry of Digital Transformation, Ukraine has foreseen a flexible approach to AI regulation. This will aid the ICT community in Ukraine in developing better AI solutions across various fields, including elections and G2C/C2G applications of AI. For instance, the plan to introduce Sandboxes and learn from other good practices could pave the way for the creation of various opportunities linked to electoral consultation and the integration of AI.

- **Support the development of AI applications in the field of national defense:** As remarked before, Ukraine has a strong technical expertise in defense, and this is reflected in the current development of AI applications that potentially can shape its military complex. However, this technical expertise can also represent an opportunity as human capacity combined with a strong technical expertise can also lead to the development of other applications related to AI, once the war is over.

- **Adapt AI success stories cautiously:** Ukraine is strongly committed to and proud of its digital public services and e-democracy tools available at national and local levels. It is therefore not a surprise that many stakeholders in Ukraine have a particular interest in exploring the use of AI for public services and elections as well as related success cases abroad. However, such practices could be explored only if the security situation in Ukraine drastically improves after the war.

- **Use the momentum to advocate the AI regulating at global level:** In terms of regulations worldwide, Ukraine is well-positioned to provide concrete quality inputs for AI regulations. Given its status of EU candidate country, Ukraine has a particular interest in implementing EU's AI Act regulations and other provisions included in other EU legislative texts. Therefore, there are plenty of other policy examples that Ukraine can replicate and adapt to its own context.

Recommendations for Ukraine

Having provided an up-to-date description of the challenges and opportunities related to AI within the Ukrainian current situation, we offer a set of short, medium, and long-term policy recommendations on the use of artificial intelligence in electoral processes especially in the context of European integration and transposition of the AI Act into Ukrainian legislation.

The scope of the following recommendations is to offer Ukrainian policy makers and civil society inputs on how to tackle concrete risks related to AI & elections as well as provide additional opportunities for Ukrainian citizens and civil society. Finally, these recommendations clustered by implementation period suggest a path for adapting EU AI policies and regulations in Ukraine.

Building a conducive environment for future AI regulation

Transparency and accountability are two key concepts that Ukrainian policymakers should follow in regulating AI in the first place, particularly in the field of electoral consultations. Hence, we have foreseen three different but related recommendations for different actors. Moreover, once Ukraine begins the transposition of AI Act into Ukrainian legislation and its operationalization, it is important to ensure that the institutional competencies related to AI regulation are ensured as per recommendations in the AI Act. Therefore, this set of recommendations is suggested to be implemented in the short term.

1) **Pilot AI before introducing any longstanding AI-technologies in elections:** Given the current political and societal context related to the Russian aggression and the current martial law, it is premature to implement any AI-powered instruments for the electoral process in Ukraine. However, piloting such tools well in advance of elections can be a valuable learning opportunity and help the Ukrainian government better understand risks and opportunities related to the use of AI in elections.

2) **Counter the use of AI for disinformation**: Given that malign actors can use AI systems to spread disinformation, it is crucial to design and implement strategies to mitigate this threat. This can include information campaigns on detecting and verifying AI-generated content, improved cooperation with for-profit and non-profit actors that work to fight AI-powered disinformation and independent fact-checkers, establishment of a trusted flaggers community that can detect disinformation content and refer it to government and/or digital platforms, exchange of experience with big tech companies that are committed to preventing the spread of disinformation on their platforms, and development of regulatory sandboxes for AI startups.

3) **Introduce soft law mechanisms for the responsible use of AI:** We encourage Ukrainian policymakers, such as the AI expert committee and the Ministry of Digital Transformation, to continue working on the development of transparency and accountability mechanisms related to AI and electoral procedures, in line with the previous examples implemented in the Roadmap and the Guidelines for media company. This can include further recommendations and guidelines for the ethical and responsible use of AI in different areas, which can act as soft law before the AI regulation is introduced.

4) **Improve general AI understanding and literacy among the public authorities:** We recommend Ukrainian public authorities to start preparing to the future applications of AI for e-government and, more specifically, G2C/C2G applications and platforms. For instance, organizing AI trainings for staff and technical personnel of public institutions in cooperation with international organizations and

donors can effectively improve capacity building both at the national and sub-national level. Ukrainian and EU experts and trainers could be invited to hold capacity building activities targeted at developing the skills and knowledge on using AI in public sector by applying blended learning approach (e.g. face-to-face and online learning format). It is recommended to involve various profiles of experts coming from public sector, civil society, private sector, academia, and media to cover multiple aspects of AI in e-government and possible future elections.

5) **Research more the Ukrainian cases:** Various organizations, such as Oxford Insights[39], CISCO[40], and the IMF[41], have created maps to show how ready different countries are for AI. These efforts are impressive, but comparing countries can be difficult because AI is a new and complex technology. In Ukraine, this task is even harder because much of the data relates to war technologies and is not available to the public. Additionally, the war has caused many people to leave their homes and has reduced the country's human resources, making it even more challenging to assess Ukraine's AI readiness. Therefore, it is recommended that academic and research institutions in Ukraine focus more on studying AI in Ukraine to better understand its true preparedness for AI adaptation.

6) **Address gender issues in the field of AI:** Technological companies, vendors, and academia should ensure that ML models do not contain gender-biased data and or would not create gender-imbalanced content while developing new products for citizens, voter and election commissioners education. In addition, civil society plays a crucial role in promoting gender-sensitive educational opportunities in the field of AI by actively raising awareness of critical issues like data bias. By addressing these challenges, vendors, academia, and civil society can influence ML applications across various sectors, including electoral processes, thereby fostering more inclusive and equitable advancements in AI technology.

Enhancing collaboration between the public and private sector

The next recommendation, which is classified as medium-term, is related to the involvement of the private sector in developing AI-powered tools for the benefit of the public sector and future elections. We recognize that the concrete implementation of transparency measures can be particularly complicated to be implemented during the war time and Ukrainian public authorities may have other priorities, as outlined in the paragraph 3 of this report. Therefore, we foresee a potential role for Ukrainian private sector to support both government and civil society in their initiatives to ensure AI transparency and accountability.

1) **The MDT should engage with public authorities and civil society:** As AI has the potential to radically shape the future of political decision making process as well as the functioning of civil society engagement, we advise businesses and startups working in the AI field to approach and engage with both public authorities and civil society in every activities that can potentially raise awareness and support AI capacity building, particularly in the field of e-government as well as G2C/C2G. For instance, awareness campaigns, projects with schools and other training within the public sector can be a good way to engage with public authorities and civil society. An effective engagement with both the public sector and citizens can also provide new business opportunities and investment opportunities for start-up and business as well.

2) **Govermental institutions should ensure transparency and countering disinformation efforts:** As AI is currently changing how disinformation techniques are run and developed, it is imperative that

39 "Release: 2023 Government AI Readiness Index reveals which governments are most prepared to use AI." https://oxfordinsights.com/insights/release-2023-government-ai-readiness-index-reveals-which-governments-are-most-prepared-to-use-ai/

40 Cisco AI Readiness Index. https://www.cisco.com/c/m/en_us/solutions/ai/readiness-index.html#blade_introduction

41 "Mapping the World's Readiness for Artificial Intelligence Shows Prospects Diverge." https://www.imf.org/en/Blogs/Articles/2024/06/25/mapping-the-worlds-readiness-for-artificial-intelligence-shows-prospects-diverge

companies involved in AI adhere to stricter transparency and accountability measures. Therefore, we invite Ukrainian companies developing AI tools (such as GPAI) to develop code of conducts and transparency mechanism to collaborate with public and private actors to ensure that transparency and that public are aware of AI-generated or AI-altered content, particularly when this is politically sensitive and have implications on the functioning of democracy. For instance, voluntary commitments and disclosure of AI-generated content can be an effective way to ensure transparency. One possible way to ensure transparency is to improve labeling for content that can potentially impact on electoral process. For instance, both sponsors of political advertising (political parties, candidates, and/or their supporters) and providers of political advertising (digital platforms) can commit to explicitly label any content generated or significantly altered by AI. This label should be displayed, making it immediately clear to the audience that the content they are reading or viewing is AI-generated or AI-altered.

3) **Take part in Sandboxes:** While Ukraine has for the moment limited opportunities to engage in testing sandbox, the EU AI Act has developed a set of potential opportunities for companies to test AI functionalities and other technical aspects in the so-called "sandboxes" which are control testing environment in which startups and other can test functions and other technical aspects related to data protection, generation of outputs etc. Therefore, we invite companies in Ukraine that work in GPAI and other technical aspects of AI that have potential implications to elections to test their functionality in sandboxes, even those established in EU member states to comply with current provisions of the AI Act that, in future, will be incorporated into Ukrainian legislation.

4) **Collaborate with domestic and global tech sector:** The CEC should collaborate closely with technology experts and policymakers to ensure that AI technologies are used ethically in elections. This includes participating in discussions on national and international platforms to stay updated on best practices and new regulatory requirements. In addition, it is recommended to establish the escalation channels between the CEC and global digital platforms to maintain crisis communications on AI-generated content, misinformation and disinformation.

Ensuring accountability and risk mitigation strategies before adopting the legislation on AI

When it comes to ensuring accountability **it is advisable for Ukraine to align with the scope of EU acquis as outlined in the Digital Services Act, Digital Markets Act, European Media Freedom Act, Transparency and Targeting of Political Advertising Regulation, and the anti-SLAPP Directive** before proceeding with the adoption of regulatory legislation on AI and its specific use in elections. This alignment will provide a robust framework ensuring that any future AI-specific regulations in the electoral context are well-founded and in harmony with established European standards. Those preparatory steps will facilitate the development of a comprehensive and coherent digital governance structure aligned with EU standards. In this context, we suggest three different non-exhaustive recommendations for the Ministry of Digital Transformation (MDT), Central Election Commission (CEC), and other policy stakeholders involved in digital transformation and elections in Ukraine that should be implemented in short- and medium-term perspective.

5) **The CEC should prepare a White Paper to analyze the risks and opportunities related to AI in elections:** As we consider the implications of artificial intelligence on Ukraine's electoral processes, it becomes clear that the current AI Act's risk-based system may not fully capture the nuances of election-related technologies, especially, taking into account the conditions of the post-war elections in Ukraine. We suggest that the CEC explore the intersection of AI and elections in Ukraine. This exploration could take the form of a comprehensive white paper, delving into the various AI technologies that touch on Ukrainian electoral system throughout the electoral cycle - from the pre-electoral, through the electoral, and into the post-electoral period. The white paper should contain specific tailored recommendations on the strategy of mitigating AI risks. The document should be

developed jointly by the government and the non-governmental stakeholders, including civil society, think tanks, private sector, media, and academia.

6) **The CEC should identify AI-related considerations in its crisis communication strategy:** This enhanced strategy should adopt a risk-oriented approach, inspired by the AI Act, to swiftly address disinformation during elections. It's crucial to establish clear transparency requirements for AI-generated content from candidates and for AI systems designed to influence voter behavior. Simultaneously, the CEC should launch a public awareness campaign to inform Ukrainian citizens about AI's potential impact on future elections. This multifaceted approach will enable the CEC to proactively manage AI-related risks, maintain electoral integrity, and foster public trust in Ukraine's democratic processes.

7) **The MDT should review personal data protection legislation to adhere to EU standards:** While it is not strictly linked to AI, Ukraine should review its data protection legislation, develop a comprehensive set of laws that fully transposes GDPR to its national legislation and ensures that accountability mechanisms are in place. This new set of regulations should also have stronger data protection component with regards to electoral purposes that can, in a later stage, be used by AI systems. Indeed, the relationship between data protection and AI risk mitigation strategies needs to be addressed in future policy reforms on electoral procedures in Ukraine.

8) **Ensure that every AI integration in the Diia app and other G2C/C2G systems are aligned with the EU standards:** While Ukrainian strategy is currently different than the EU one in terms of AI regulations and the AI Act won't have immediate implications for Ukraine, it is also true that the process of integration of Ukraine into the EU will require the transposition of the AI Act to its national legislation and, ultimately, its enforcement and adequate implementation mechanism. As Ukraine is already quite advanced in providing e-government services, it would be useful to ensure that the Diia App and other G2C/C2G systems implemented in the country follow the AI Act when it comes to integration with AI systems and risks mitigation strategies. This will facilitate the integration into the EU in terms of expertise and capacity to implement technical reforms.

Capacity building and training

Overall, Ukraine is well positioned to take advantages in the field of AI and elections in the medium and long term, however there are certain issues that require stronger investments in terms of human capacity, particularly in areas related to AI knowledge and technical expertise in the public sector. Hence, three recommendations should be followed simultaneously with the previous set of recommendations in the short, medium, and long-term period.

1) **Increase the technical understanding of AI in the public sector:** While in the Ministry of Digital Transformation there is generally a strong knowledge of AI implications, there is a strong need to organize capacity building and trainings in other ministries and public bodies to take full advantages of AI transformation and how the public sector can develop initiatives related to G2C/C2G that can fully benefit citizens. Therefore, it is imperative to organize more technical AI trainings for those who work in ministries and public bodies, especially those election-related stakeholders such as the election administration bodies, the Central Election Commission (CEC), and the National Agency on Corruption Prevention (NACP).

2) **Improve general understanding of AI related to elections:** While we do not foresee any form of voting during the martial law (traditional or electronic), we believe that Ukrainian people at large need to be better prepared to fully understand the risks and opportunities associated with AI, with a particular focus on disinformation campaigns such as deepfake and misleading AI-generated content. Hence, more educational campaigns in this field should be organized by involving civil society and

educational institutions. At the same time, improving capacity building in this field can be a potential area of cooperation with donors and international organizations interested in strengthening Ukrainian society at large.

3) **Replicate good practices implemented in other countries:** The Ukrainian policymaking has shown an incredible commitment and resilience to launch a Roadmap and other key documents in the field of AI while a full-scale Russian aggression is taking place. At the same time, it is also true that the resources and policy initiatives related to initiatives other than security and defense are limited. Hence, mapping and replicating good practices in the field of AI related to elections and electoral procedures can be the key to ensure that the best educational and technical resources are available for people involved in policymaking. By replicating success stories and other best practices in this field, especially in the EU, Ukrainian public sector can effectively achieve more and better results in the field of AI and elections.

4) **Implement the OODA Cycle for using AI in electoral processes:** To effectively integrate AI in elections, it's recommended for the CEC to utilize the OODA (Observe, Orient, Decide, Act) cycle, beginning with robust monitoring of global AI developments in electoral contexts. This involves gathering insights on AI's performance and applicability in elections, focusing on identifying potential opportunities and risks relevant to Ukraine's electoral framework. The orientation phase should analyze this data to customize AI solutions that align with Ukraine's electoral needs and socio-political landscape. Informed by this analysis, strategic decisions about suitable AI technologies for pilot testing can be made by the CEC, prioritizing those that enhance electoral integrity and are compatible with existing infrastructure. Throughout this process, it is important to maintain a continuous feedback loop, collecting and analyzing stakeholder feedback to iteratively refine and optimize AI applications, ensuring the technology meets the evolving needs and maintains electoral transparency. CEC is advised to develop and use AI tools that fall under the non-high-risk category for administrative and logistical tasks in electoral management. These tools should not directly influence voter decisions but can enhance the efficiency and transparency of the electoral process.

5) **Develop educational and awareness programs:** CEC should develop educational programs to raise awareness among electoral stakeholders, including voters, about the role of AI in elections. This would include information on the benefits and risks associated with AI, fostering an informed electorate that understands how AI tools are used in electoral contexts.

Annex 1. Short Literature Review

For the convenience of our readers, we present here a non-exhaustive list of policy documents that we highly recommend for further reading. Our aim is to showcase how the policy discourse on AI and elections has generated a range of compelling documents that address various aspects discussed in this report. We are also convinced that while the efforts to regulate AI and adopt effective democratic and policy-driven solutions in areas related to elections may still seem quite challenging, several resources are available. Therefore, Ukrainian policymakers, civil society, and stakeholders can find inspiration and explore good practices and policy solutions that have been developed worldwide to complement the policy recommendations that we have elaborated in the previous chapter.

- European Commission's White Paper on "Artificial Intelligence: A European Approach To Excellence And Trust"[42] (2020). This is the first white paper that the EU has developed in the field of AI and analyses a series of implications for the EU member states. For example, it highlights how the EU is positioned to benefit from AI technological development and to what extent joint efforts at the EU level are needed in the field. It also highlights that the governance structure relating to AI and the possible conformity assessments should be a priority for the EU, particularly in the private sector and in terms of international cooperation.

- European Union Strategy on Artificial Intelligence[43] (2020). This document, drafted by the European Commission, highlights the strategic principles of AI regulation for European policymakers. It emphasizes the necessity of developing a regulatory approach to AI that benefits people and society as a whole. For example, it stresses the importance of the EU stepping up investments to strengthen fundamental research and make scientific breakthroughs. Additionally, it underscores democratic principles such as inclusion, sustainable progress, and ethical considerations related to AI.

- European Union's Coordinated Plan on Artificial Intelligence Review[44] (2021). The 2021 Coordinated Plan on Artificial Intelligence is an EU document aimed at attracting post-Covid investments in AI technologies to drive resilient economic and social recovery, remove fragmentation, and address global challenges in the field of AI. It also includes a Proposal for a Regulation on Artificial Intelligence that was later reflected in some elements of the AI Act.

- European Commission's Study on "The impact of new technologies on free and fair elections"[45] (2021). This document provides an overview and analysis of pertinent literature identified and reviewed within the framework of a study on the influence of emerging technologies on the integrity of electoral processes. The primary aim of this study is to investigate the utilization of voter data and advancements such as micro-targeting techniques, algorithms, e-voting, and AI in shaping election outcomes and public trust. In particular, it delves into the incorporation of AI within EU legislation and explores its practical implications for electoral procedures.

42 "White Paper on Artificial Intelligence: a European approach to excellence and trust." https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

43 European Union Strategy on Artificial Intelligence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN

44 Coordinated Plan on Artificial Intelligence 2021 Review. https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

45 European Commission's Study on "The impact of new technologies on free and fair elections." https://commission.europa.eu/system/files/2022-12/Annex%20I_LiteratureReview_20210319_clean_dsj_v3.0_a.pdf

- OSCE Policy Paper on "Artificial Intelligence's (AI) Impact on Freedom of Expression in Political Campaign and Elections"[46] (2021). This OSCE Policy Paper discusses how AI affects freedom of expression in political campaigns and elections. It suggests adopting human rights principles in policies to protect freedom of expression within the OSCE area. The paper also offers recommendations to influence upcoming AI regulations at the EU and international levels and provides a technical framework to help organizations study AI and social media's impact on freedom of expression in politics.

- University of Surrey's Institute for People-Centred AI's Report on AI And Elections: Are We Ready To Save Democracy?[47] (2023). In this short policy document, experts from the University of Surrey's Institute for People-Centered Artificial Intelligence (AI) and Department of Politics examine trends that may be leveraged by campaigns using AI to disrupt and influence the outcome of various elections in 2024. Their primary conclusion is that there is no universal "quick fix" to this issue, given that the 2024 elections are already underway worldwide, making it neither feasible nor desirable to ban Generative AI. While they propose a set of solutions for the UK, they also emphasize the importance of holding platforms accountable for AI-generated content worldwide.

- The University of Chicago - Harris School of Public Policies' report on "Preparing for Generative AI in the 2024 Election: Recommendations and Best Practices Based on Academic Research"[48] (2023). This white paper is the outcome of a collaborative effort between the University of Chicago Harris School of Public Policy and the Stanford Graduate School of Business. In its policy recommendations, it advocates for campaigns and political parties to openly commit to refraining from utilizing deceptive AI-generated content in their campaign materials. Moreover, the paper urges tech companies to ensure that chatbots clarify their limitations as reliable sources of technical election information and redirect users to trusted websites.

- United States of America's National Artificial Intelligence Research and Development Strategic Plan[49] (2023). This strategic document is part of the Biden administration's efforts to outline a National Artificial Intelligence Research and Development Strategic Plan. The policy document was crafted by the US Committee on Artificial Intelligence and it delineates nine strategic domains for implementing policy activities within the US. A key aspect emphasized is Cultivating a Global Culture of Developing and Using Trustworthy AI, which is also the final strategic plan reported. This topic underscores the significance of fostering transparent, democratic, and mutually agreed-upon AI principles with partner countries and facilitating exchange of ideas and good practices in the AI field.

46 OSCE Policy Paper on "Artificial Intelligence's (AI) Impact on Freedom of Expression in Political Campaign and Elections." https://www.osce.org/files/f/documents/a/3/483638.pdf

47 University of Surrey's Institute for People-Centred AI's Report on AI And Elections: Are We Ready To Save Democracy? https://www.surrey.ac.uk/sites/default/files/2024-03/ai-and-democracy-policy-paper.pdf

48 The University of Chicago - Harris School of Public Policies' report on "Preparing for Generative AI in the 2024 Election: Recommendations and Best Practices Based on Academic Research." https://harris.uchicago.edu/files/ai_and_elections_best_practices_no_embargo.pdf

49 United States of America's National Artificial Intelligence Research And Development Strategic Plan. https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

Annex 2. Stakeholder Map: Elections and Artificial Intelligence in Ukraine

Title	Type	Description of the activity
Central Election Commission[50]	Public institution	A permanent and independent governmental body that is responsible for organizing the arrangements of the presidential and parliamentary elections in Ukraine as well as the local elections at all levels, managing the all-Ukrainian and local referendums according to the procedure and within the legal framework defined by the laws of Ukraine.
Ministry of Digital Transformation[51]	Government	The Ministry of Digital Transformation is responsible for a wide range of digital and technological initiatives in Ukraine. It ensures the development and implementation of state policy in several key areas such as artificial intelligence, digital economy, digital innovations, e-governance, and e-democracy, as well as the development of the information society. It is tasked with forming and implementing state policy for developing digital skills and digital rights of citizens.
National Council on TV and Radio[52]	Public institution	The National Council on Television and Radio Broadcasting oversees compliance with Ukrainian laws in the field of television and radio broadcasting and exercises regulatory powers as stipulated by these laws. It also registers online media and acts as a state regulatory body for video-sharing platforms.
Ministry of Culture and Information Policy[53]	Government	The Ministry is responsible for shaping and implementing state policy across several crucial areas. Among other responsibilities, the Ministry is tasked with safeguarding Ukraine's information security, a critical aspect in today's digital age. This involves protecting the country's information space from potential threats and ensuring the resilience of its information infrastructure.

50 The Central Election Commission of Ukraine. https://cvk.gov.ua/en
51 The Ministry of Digital Transformation of Ukraine. https://thedigital.gov.ua
52 The National Council on Television and Radio Broadcasting of Ukraine. https://webportal.nrada.gov.ua/en
53 The Ministry of Culture and Information Policy of Ukraine. https://mcip.gov.ua/en

Title	Type	Description of the activity
National Security and Defence Council under the President of Ukraine[54]	President of Ukraine	The National Security and Defense Council of Ukraine (NSDC) is a coordinating body for national security and defence matters under the President of Ukraine. According to the Constitution of Ukraine, the NSDC coordinates and oversees the activities of executive bodies in the sphere of national security and defense. It supervises the National Coordination Center for Cybersecurity and also the Center for Countering Disinformation which ensures the implementation of measures to counter current and projected threats to Ukraine's national security and national interests in the information sphere.
Committee on State Building, Local Governance, Regional and Urban Development[55]	Parliament	The Committee is responsible for a wide range of digital and technological matters in Ukraine. Its areas of focus include the legislative foundations for digitalization and digital society, national and state information programs, and participation in EU digital initiatives such as the Digital Single Market, GDPR, etc. The Committee oversees innovation in digital entrepreneurship, startup ecosystem development, and research centers in digital technologies. It also covers development of legislation for digital industry and telecommunications, e-governance and public electronic services, e-democracy, electronic trust services, and digital identification.
Committee on Human Rights, Deoccupation and Reintegration of Temporarily Occupied Territories, National Minorities and Interethnic Relations[56]	Parliament	The key areas of focus are related to human rights and legal protections in Ukraine. It deals with legal regulation of civil rights and freedoms, as well as incorporating European standards for these protections into national law, developing legislation regarding the collection and use of personal data, excluding specific protections for information and personal data in digital systems.
Committee on Freedom of Speech[57]	Parliament	The Committee is responsible for several key areas related to media and information rights in Ukraine. Its primary focus is on ensuring freedom of speech and protecting citizens' rights to information. The Committee works to safeguard the rights and freedoms of media workers, including journalists and other professionals in the field. It also oversees the guarantees for media operations, ensuring that media outlets can function freely and independently.

54 The National Security and Defense Council of Ukraine. https://www.rnbo.gov.ua/en

55 Committee on State Building, Local Governance, Regional and Urban Development. https://komsamovr.rada.gov.ua

56 Committee on Human Rights, Deoccupation and Reintegration of Temporarily Occupied Territories, National Minorities and Interethnic Relations. https://kompravlud.rada.gov.ua

57 Committee on Freedom of Speech. https://komsvobslova.rada.gov.ua

Title	Type	Description of the activity
National Agency on Corruption Prevention[58]	Government	A national anti-corruption agency of the Ukrainian government which is responsible for shaping and implementing anti-corruption policy, while creating an environment conducive to corruption prevention.
Expert Advisory Committee on the Development of Artificial Intelligence in Ukraine[59]	Government	The Expert Advisory Committee on the Development of Artificial Intelligence in Ukraine under the Ministry of Digital Transformation of Ukraine was established on 21.12.2019 (Order No. 28). The main task of the Committee is to increase Ukraine's competitiveness in the field of artificial intelligence.
Civil Network OPORA[60]	NGO	A non-governmental organization and watchdog that works to develop practices of responsible decisions and actions through the advocacy of fair rules to enhance security and democracy in Ukraine.
Center of Policy and Legal Reform[61]	NGO	A non-governmental organization and think tank which is focused on developing and facilitating reforms that will ensure democracy and the rule of law in Ukraine and lead it to EU membership in the future.
The Institute of Innovative Governance[62]	NGO	A non-governmental organization and think tank established in 2018 that aims to provide innovative solutions to governance issues in Ukraine through inclusive digital transformation and emerging technologies, protection of digital rights, and combating disinformation.
Digital Security Lab[63]	NGO	A non-governmental organization and think that aims to protect digital rights and ensure information and cyber security in Ukraine.
Internews Ukraine[64]	NGO	A non-governmental organization focused on media development, strategic communications, and information security since 1996. The organization works on various projects to increase media literacy, support independent media, and protect Ukraine's information space.
StopFake[65]	NGO	A specialized resource for combating false information about events in Ukraine. They identify and refute fake news, manipulations, and other types of information attacks.

58 National Agency on Corruption Prevention of Ukraine. https://nazk.gov.ua/uk/
59 Expert Advisory Committee on the Development of Artificial Intelligence in Ukraine. https://ai.org.ua/
60 Civil Network OPORA. https://www.oporaua.org/en
61 Center of Policy and Legal Reform. https://pravo.org.ua/en/about/
62 The Institute of Innovative Governance. https://instingov.org/en/
63 Digital Security Lab. https://dslua.org/about/
64 Internews Ukraine. https://internews.ua/
65 StopFake. https://www.stopfake.org/ru/glavnaya-2/

Title	Type	Description of the activity
Detector Media[66]	NGO	An independent Ukrainian media project that focuses on media monitoring, media content analysis, disinformation detection, and research in the field of media communications and media literacy. The project is actively working to raise the level of media education among citizens and promotes the development of independent media in Ukraine.
Ukrainian Foundation for Security Studies[67]	NGO	UFSS is a non-governmental think tank specializing in national security issues, with a focus on communication and information security. The organization develops and implements projects aimed at strengthening Ukraine's information sovereignty.
The Centre for Democracy and Rule of Law[68]	NGO	CEDEM is a non-governmental think tank focused on democracy and the rule of law. The organization implements projects in the areas of access to information, independent media, public service broadcasting, and support for civil society.
CAT-UA (Communication Analysis Team - Ukraine)[69]	NGO	It started as a volunteer team providing media analysis to support the Ukrainian authorities during the full-scale invasion. Now it has evolved into a non-governmental organization that conducts research to combat manipulation and information special operations, aimed at creating transparent and modern communication principles in Ukraine and abroad.
Mantis Analytics[70]	Start-up	An AI-driven real-time information field monitoring platform.
Osavul[71]	Start-up	A software development company that focuses on creating artificial intelligence solutions to protect governments, businesses, and society from information threats. The main areas of focus include information environment assessment, protection against disinformation and coordinated misbehavior.
Semantrum[72]	Start-up	A media monitoring and reputation analytics platform that allows round-the-clock monitoring of online mentions in real time, using artificial intelligence to analyze the tone of mentions, identify brands, individuals, and geographic locations from a data set of more than 50,000 sources.
Content Analysis Center[73]	Company	A Ukrainian consulting company that specializes in monitoring the media space, analyzing content, and providing professional recommendations for companies. The organization offers research of any complexity, developing terms of reference for the client's needs, and recommends comprehensive solutions for various business segments.

66 Detector Media. https://detector.media/
67 Ukrainian Foundation for Security Studies. https://ufss.com.ua/
68 The Centre for Democracy and Rule of Law. https://cedem.org.ua/
69 CAT-UA (Communication Analysis Team - Ukraine). https://cat-ua.org/
70 Mantis Analytics. https://mantisanalytics.com/
71 Osavul. https://www.osavul.cloud/
72 Semantrum. https://www.world.semantrum.net/
73 Content Analysis Center. https://ukrcontent.com/

Annex 3. Leveraging AI In Elections Through Electoral Cycle

DIMENSION	ELECTORAL CYCLE PERIODS		
	Pre-electoral	Electoral	Post-electoral
Narrative:	The focus is largely on planning, training and awareness raising, information sharing, and registration efforts	The focus is on nominating, campaigning, voting, results tabulation and announcement, as well as complaints handling	The focus is on audits, reviewing, analyzing, reforming, and strategizing an election
Technical	• Detect and flag duplicate or repeated voter registrations • Filtering tools to search for missing, incomplete, or incorrect data • Compare registration information with other sources of official documentation or historical data • Polling site locations and resource allocation • Election baseline estimation: election costs forecasting, campaign expenditures, voter turnout rates, and election results; electoral security/ violence prediction	• Detect and summarize common election misinformation • Detecting specific social media posts that violate election laws • Fact-checking • Verifying voter identification documents • AI-based optical character/ mark recognition • Biometric (e.g., eye, face, palm, thumbprint) recognition for voter verification • Detecting polling place incidents (reports of polling place incidents) • Vote tabulation through the recognition of filled-in and written forms • AI-based signature matching tools • Real-time turnout analysis for detecting potential anomalies	• Post-election auditing • Evaluate the efficiency and resource allocation of various polling sites • Consolidating various campaign expenditures and donations into standardized formats • Tracing political donations and expenditures

DIMENSION	ELECTORAL CYCLE PERIODS		
	Pre-electoral	Electoral	Post-electoral
Perceptual	• Tailoring election information to specific subsets of the population • LLM chatbots • Targeted advertising to increase voter turnout or distribute election information to diverse social groups • Using GenAI tools to modify ads according to users' personality	• Detect trends in misinformation and disinformation and flagging the most concerning cases • Fact-checking tools • Monitoring of the campaign silence period • Detection of violent speech and gender bias	• Consolidation and auditing of political finance documents and reports • Detection of incidents or fraud
Risks	• Uninterpretable AI approaches used without human oversight • Inaccurate models • Lack of transparency • Risk of wrongfully removing eligible voters • Serious concerns regarding data privacy, manipulation, and accuracy	• Missing key topics and concerns, especially on private messaging platforms (e.g., Telegram) • Lack of clear understanding of what constitutes misinformation • Violation of the rights to free speech • Concerns about surveillance and government monitoring of public media platforms • Models may perform in a discriminatory manner	• Lack of trustworthy data from the ground • AI tools used to consolidate data may suffer from hallucinations or other accuracy concerns

HQ 2011 Crystal Drive | Arlington, VA 22202 | USA
www.IFES.org