Abstract. The malicious use of deepfake technology can lead to violations of human rights and freedoms, or even facilitate criminal activities such as financial fraud. However, creating manipulated images can also pose other threats, including those to democratic states and the principles that govern them. The upcoming presidential elections in the United States and the recent parliamentary elections in European and non-European countries have delivered an impulse for a discussion on the impact that deepfake can have on elections, on the ethics of holding elections and on the principles of democracy, on how countries fight these threats, and on how sufficient and effective the implemented methods really are.

Keywords: deepfakes; elections; democracy; disinformation; manipulation.

INTRODUCTION

Deepfake may take the form of an image or sound manipulated using artificial intelligence that shows behaviour or statements of a person who has never behaved in a given way or uttered specific words. The threats resulting from creating false images are usually considered in terms of violation of human rights, especially the right to privacy or the right to good reputation. Unauthorized use of someone's image often involves compromising the person's reputation. The most high-profile cases involved famous people whose images were used to create pornographic deepfakes [Gosse and Burkell 2020, 497]. The use of deepfakes was also often used for criminal activities, for example financial fraud. The literature describes cases in which audio recordings prepared using deepfake technology were used to mislead an unsuspecting person, who then transferred money to the account indicated by the fraudster. One of the most striking examples is probably the case from Hong Kong, where bank employees made transfers for a total of USD 35 million, thinking that they were taking orders from the branch manager

1 Gosse and Burkell pointed out that 90-95% of all deepfakes on the Internet may have a pornographic nature.
[Ghandi and Sharma 2023]. However, another danger posed by misused deepfake technology is a threat to democratic systems otherwise free from electoral manipulation. Electoral manipulation and disinformation have now become extremely common and have accompanied many elections, both European and non-European, for years. This year, over 40 different types of elections are planned to be held globally, ranging from presidential, to parliamentary and finally to local government elections. The possibility of using deepfake technology only intensifies the potential threat of disinformation and makes the holding of manipulation-free elections seem a major challenge now.

Cases of use of deepfakes in election campaigns in many countries are common. Suffice it to mention the recent elections in Indonesia, when voters, using deepfakes, had the opportunity to see and hear the late President Suharto, who encouraged them to vote [Culloty 2024]. This recording was considered unethical due to the fact that it was generated by the political party that the deceased had headed during his life. Another example is last year’s parliamentary elections in Slovakia, where during the election campaign, two days before the vote, a voice recording appeared on Facebook in which the leader of the Progressive Slovakia party, Michal Šimečka, allegedly talked to a journalist about election fraud [Meaker 2023]. A similar procedure was used in February 2023 during elections in Nigeria against one of the presidential candidates [Mirza 2024]. Deepfakes were also distributed on a large scale in Taiwan, where the target of the attack was Ko Wen-je, one of the presidential candidates from the Taiwan People’s Party [Lau 2024]. Deepfakes were also used during the last elections in India, where on the eve of the vote a recording was released in which the President of Delhi State Manoj Tiwari from BJP allegedly criticized his political opponent. The actual recording that was manipulated involved Twari speaking on a completely different topic [Safullah and Parveen 2022, 256]. These numerous examples from different countries only prove that the problem is extremely serious and global.

Deepfakes are used in the ongoing presidential campaign in the United States. While fake news was spread and manipulated in the course of previous election campaigns, currently the United States must face a new technology that escapes all existing legal regulations. In February 2024, President Joe Biden himself fell victim to deepfakes, when using this technology an audio recording very similar to the president’s real voice was generated, in which he allegedly urged his voters not to take part in the primaries organized in New Hampshire. This recording was then distributed through two telecommunications companies in Texas: Life Corporation and Lingo Telecom using robocalls [Leinigang 2024]. Steve Kramer, a consultant to the staff of Dean Phillips – Joe Biden’s opponent in the Democratic
primaries – admitted to the idea of preparing and disseminating a deepfake. He pointed out that he had acted independently, and his actions, although at the peripheries of ethical behaviour, resulted in a campaign worth several million dollars at a much lower cost.²

This case (although there is no confirmed data on how many people actually did not take part in the primaries after receiving the generated and spread deepfake) shows how easy it is now to spread information chaos on a large scale. Specialists and voters themselves were involved in generating fake news in the previous presidential elections (both in 2016 [Bovet and Makse 2019, 1-14] and 2020 [Starbird, DiResta, and DeButts 2023, 1-17]), which mostly meant that they produced and then shared on a massive scale false information on their social media profiles (including Facebook-Meta, Instagram, Twitter). Currently, at very low costs and using AI, political opponents are able to achieve much better results in reaching potential recipients than using “traditional” social media. This fact makes the use of the latest technologies with malicious intentions a very serious threat to the entire electoral process and the principles of democracy.

Taking all this into account, the aim of this publication is to present what impact deepfakes may have on elections, on the ethics of holding them and on the principles of democracy, on how countries fight these threats and on how sufficient and effective the methods implemented really are.

1. THE IMPACT OF DEEPFAKES ON ELECTORAL PROCESSES

The use of deepfake technology to manipulate the electoral process carries basically similar threats to the electoral process and democracy as the creation and dissemination of fake news using already known techniques, e.g. bots. This is because, although the manipulation technique is different, it is still false information intended to intentionally mislead the recipient. However, it should be noted that although the threats generated by fake news and deepfakes may be the same, the effects of the latter are much more serious.

Firstly, it is because it is increasingly difficult now to distinguish real recordings from images and sounds manipulated using AI. The technique of creating deepfakes is almost so perfect that research shows that most people are unable to distinguish a recording depicting real events from a synthetically produced one [Köbis, Doležalová, and Soraperra 2019, 1-18]. Moreover, there is no widely available tool that would allow anyone to check

the authenticity of an image or audio. Secondly, the reach of deepfakes is much wider, because they can be spread in various ways, not only online, as in the case of “traditional” fake news. Thirdly, deepfake technology is very easily available, anyone can use it without having to incur large financial outlays [Pawelec 2022, 3]. Fourthly, content generated using AI can affect the recipient with a much greater impact than the content so far created by paid people, because Artificial Intelligence is able profile the content recipient much more easily than a human being who does not know the recipients’ cultural context well [Goldstein, Sastry, Musse, et al. 2023, 2]. And finally, fifthly, an appropriate tool has not yet been created that would help identify deepfakes and remove them while signalling to recipients that the content has been manipulated (such tools exist for traditionally manipulated information posted on social media, e.g. Facebook – Meta, Instagram, or Twitter) [Tan 2022, 513-36]. All this means that in the face of deepfakes, the existing legal basis and IT tools are helpless, and society’s distrust in the information presented to them increases [Olan, Jaywickrama, Arakpogun, et al. 2022, 443-58].

The widespread occurrence of fake news, social bots and now deepfakes in the public space forces recipients of messages to be vigilant and to verify every piece of information that could have been accepted with faith in its authenticity before the era of computerization of society. This significantly hinders access to information, which not only is provided by democratic constitutions, but is also guaranteed by international legal acts, such as the Universal Declaration of Human Rights or the Convention for the protection of human rights and fundamental freedom. Ultimately, this situation may lead to two extreme behaviours – excessive distrust and the need to verify every piece of information, or excessive gullibility, also caused by the lack of appropriate tools to verify facts. Both behaviours do not only have a negative impact on social relations [Al-Khazraji, Saleh, Khalil, et al. 2022, 429-41], between representatives of authorities and citizens or between private individuals in everyday contacts, but they also have a great impact on people’s voting behaviour.

The spread of false information on the Internet using deepfake technology significantly contributes to the possibility of manipulation in elections [van der Sloot and Wagensveld 2022, 6]. These activities may be organized at the national level, with deepfakes targeting political opponents. With their help, public trust in the candidate may be reduced because his image and credibility may be lost. In extreme cases, this may even lead to the elimination of such a person from public life and the end of their political career.

As a rule, the onus will be on the victim of a deepfake to prove that the materials presented are not true. Barack Obama was put in such a situation, having to explain the widespread deepfake in which he was allegedly mocking Donald Trump [Chawki 2024, 6]. These behaviours should, of course, be considered unethical, because using new technologies to discredit a political opponent is reprehensible and political disputes should be resolved in a political debate, using substantive arguments by the parties. Moreover, it should be noted that a control of voters deprives them of the ability to make informed electoral decisions to which they are entitled.

Politicians also begin to manipulate the electorate when they want to force certain attitudes on their voters. We can mention here the deepfake involving Donald Trump who allegedly spoke about climate change in the context of Belgium. The recording caused a lot of emotions in Belgium and people who believed in the deepfake spoke critically of the US President for interfering in the affairs of a foreign country. In fact, it was a production created by one of the Belgian political parties, whose aim was to mobilize people in Belgium to sign an appeal calling on the Belgian government to take immediate action to combat climate change [ibid.]. Deepfakes can therefore become a tool that will shape citizens’ attitudes but they may also influence actions taken by governments and heads of state. On the other hand, they can also be used to polarize society, just as “traditional” fake news has been used for this purpose so far [Olan, Jaywickrama, Arakpogun, et al. 2022, 443-58].

Political manipulation using deepfakes can also happen at the international level. This usually happens when one country wants to achieve its own benefits by interfering in another country’s elections. The impetus for such action is primarily the specific political interests of the interfering state. An example of such activities may be China’s interference in the elections in Taiwan, when the Internet was flooded with deepfakes against a presidential candidate who opposed Chinese claims to make Taiwan part of Chinese territory. Similar methods, aimed at disinformation and weakening trust in a specific person, were used by Russia in the context of the war in Ukraine, creating and spreading a deepfake in which President Volodymyr Zelensky allegedly called for Ukrainians to refrain from fighting [Wakefield 2022]. These activities lead to information chaos, but also to a decline in public trust in other presented facts. Therefore, there is an increasing tendency in society to question even true information. All this makes such a society easier to manipulate, and foreign countries take advantage of this situation to achieve their political goals. It should be recognized that

---

traditional methods of protecting the state and politics as well as the electoral process (such as: transparency of financing of political parties, prohibition of financing political parties by foreigners, etc.) against foreign influences are therefore no longer sufficient, because foreign states currently can, with great ease, noticeably interfere in the electoral, political and social processes of other countries.

Another threat posed by deepfake technology in the context of elections and broadly understood politics is the “liar's dividend” phenomenon. This term was coined by T. Chesney and S.K. Citron, who pointed out that the more society becomes aware that both video and audio can be faked in such a way that it will be difficult to tell whether it is real or not, the more this situation can be taken advantage of by people who, wanting to avoid responsibility for their actions or spoken words, will question their veracity, claiming that image or audio recordings are simply deepfakes [Chesney and Citron 2018, 1785]. Such situations have already occurred, among others, in the context of elections in Turkey, where the disgraced candidate Muharrem İnce announced that the presented recordings, although they were in fact authentic, were only an AI-generated deepfake [de Mesquita, Canes-Wrone, Hall, et al. 2023, 6]. Such actions are very unethical and at the same time do not only violate the subjective right of access to reliable information, but also have a negative impact on the electoral process. The electorate does not have a full, real picture of the situation, which means that an electoral decision may have to be made only on the basis of trust or lack thereof in a given candidate.

2. METHODS OF COMBATING MALICIOUS USE OF DEEPFAKES

Democratic countries are aware of the threat posed by deepfakes, which is why they are fighting against their misuse, also in the electoral aspect. The range of proposed protection measures against deepfakes is extremely wide. The most stringent idea is probably to introduce a legal ban on the creation and distribution of deepfakes. Considering the threats they pose in the social, political and economic spheres, as well as the negative impact they may have on the functioning of democratic states, adoption of such a solution was considered [Songja, Promboot, Haetanurak, et al. 2023, 6]. However, no country as yet has decided to implement this measure pondering the possibility of violating the protection of fundamental freedoms and human rights, including: freedom of expression and creative freedom. A complete ban on the use of deepfakes would also eliminate those deepfakes whose use has certain social and educational benefits, such as “reviving” dead artists in museums (e.g. Dalí Museum in St. Petersbug [Mihailova 2021, 882-98]).
Another way to combat malicious use of deepfakes is to introduce restrictive legal regulations that will enable the state and its bodies to prevent the spread of disinformation. An example of such a country is China, which has introduced an obligation to always obtain the consent of the person whose image or voice is to be used in deepfakes. Moreover, Chinese legal regulations also provide for the obligation to mark deepfakes so that it is easy to find the source of the creation.\(^6\) Regulations that require that content be marked as deepfake have also been prepared in the US at the federal level.\(^7\) Apart from this, state regulations are also being created to combat disinformation in the electoral aspect. For example, Nebraska has proposed to introduce a ban on disseminating election deepfakes within 60 days before the vote [Mirza 2024]. In Virginia and California laws were passed prohibiting the creation and distribution of videos that would present false behaviour or statements of politicians. The only exception to this rule are deepfakes that constitute parody or satire, and they must clearly indicate that they are deepfakes [Wasilewski and Lenart 2020]. The US has also adopted ad hoc response tactics to threats arising from the malicious use of deepfakes. In the case of the deepfake of President Biden spread during the Democratic primaries, the Federal Communication Commission declared the use of AI-generated voices in robocalls illegal.\(^8\)

When it comes to European Union regulations, a kind of novelty in relation to the other methods already discussed is the introduction has been introduced: an obligation addressed to social media giants (e.g. Meta, Google, Twitter), which calls upon them to mark content recognized as deepfake on social media platforms.\(^9\) This means that the European Union has extended the responsibility for detecting and reporting modified videos and audio to technology companies as well.

The activities discussed above largely overlap in all countries, whether European or non-European. The most common model for combating deepfakes is the obligation imposed on creators to inform that a given material has been manipulated using artificial intelligence generators. Additionally, sometimes, as in the case of EU regulations, the information obligation is also extended to other entities. In this case, however, this method may fail. Artificial intelligence is developing faster and faster and becoming

more and more perfect. However, there are no commonly available tools that would make it possible to recognize and track deepfakes on the Internet. Only the largest companies have such generators, and even these tools do not always work flawlessly [Albahar and Almalki 2019, 3247-249]. This does not mean, however, that the actions taken are pointless. This rather shows that legal regulations alone cannot adequately protect society against the effects of deepfakes, and cooperation is also needed at the technological level. Moreover, the literature indicates the need to carry out activities to raise public awareness of the threats posed by new technologies [Chawki 2024, 1-13]. Only such a comprehensive approach may provide a chance for the fight against malicious deepfakes to be effective.

CONCLUSIONS

The electoral process, which begins from the moment the elections are announced and which consists of many interconnected stages, is extremely complex. The electoral law that regulates this process in many countries is created in such a way as to protect each stage from possible abuses, in order to protect the electoral act, as well as the voters themselves, against distortion of their will by the use of techniques of external influence [Colomina, Margalef, and Youngs 2021, 14-15]. The manipulation tools used may result in appointing a body that does not correspond to the actual will of voters. This is because some people may not verify the information and believe the fake news. Sometimes, as in the case of the elections in Taiwan, a deepfake may be spread several days before the vote, making it impossible to correct the manipulated message. It should also be noted that some dishonest politicians may claim that their behaviour or statements have been manipulated with deepfake technology, which in fact did not happen and is only intended to mislead voters.

Spreading disinformation using deepfakes also has a number of other negative effects on state democratic mechanisms. First of all, it causes a lack of social trust in state authorities, which weakens their position and prestige [Ternovski, Kalla, and Aronow 2022, 1-16]. It contributes to enabling unethical fighting between political opponents and may also lead to the polarization of society (simultaneous acquisition of new supporters and destruction of the image of political opponents). Deepfakes can also threaten the emergence of uncontrolled influence of a foreign state on political and social issues.

Controlling the integrity of the electoral process is now even more difficult due to ongoing technological development and the emergence of many new spaces for disseminating false information that may influence voters’ attitudes and final choices. The fight against the spread of deepfakes
is also difficult due to the fact that when applying certain legal or technical solutions, the authorities must also take into account other human rights and freedoms than just electoral rights (e.g. freedom of expression, the right to protest, the right to object, etc.) [Dias, Doca, and Silva 2021, 1-14]. Therefore, any restrictions they may impose on the creation and use of new technologies must be proportionate. It should be noted that the most frequently adopted legal measures, which involve the obligation to mark content created with the use of AI, are not sufficient due to the lack of effective tools for detecting deepfakes and due to the continuous development of new technologies, which means that legal provisions quickly cease to fulfil their role. Therefore, in order to protect the electoral process against manipulation (but also more broadly in the context of protecting other human rights against the threats posed by deepfakes), it is recommended that comprehensive actions based on cooperation of legislative entities of states, international entities and technology concerns be taken, while supporting public awareness by educational activities and by providing information about possible violations of law caused by deepfakes technology.

REFERENCES


Culloty, Eilee. 2024. “Deepfakes are still new, but 2024 could be the year they have an impact on elections.” https://theconversation.com/deepfakes-are-still-new-but-2024-could-be-the-year-they-have-an-impact-on-elections-224786 [accessed: 03.03.2024].


