Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215962

Deepfakes as a tool of digital manipulation and disinformation

Karolina PIĘTA
Katolicki Uniwersytet Lubelski Jana Pawła II
ORCID: 0000-0002-9036-8276
E-mail: karolina.pieta@kul.pl

Abstract

The deepfake phenomenon is one of the most advanced tools of digital manipulation in the modern information age. Technology based on artificial intelligence and deep learning allows the creation of incredibly realistic yet completely false video and audio materials that can effectively mislead audiences. The aim of this article is to present the essence of the deepfake phenomenon, and development, analyze the mechanisms of manipulation and disinformation in the context of deepfakes, and discuss countermeasures against the deepfake phenomenon, with particular emphasis on regulatory strategies and methods for mitigating the negative effects of this technology in the digital space.

Keywords

disinformation, deepfake, manipulatios, digitalization, tool of digital

Introduction

The present day is dominated by rapid technological progress, which increasingly shapes the way individuals and entire societies function. This phenomenon is leading to profound changes in everyday life, affecting the way we communicate, obtain information, spend our free time, educate ourselves, and work. Technology permeates almost every aspect of social reality, influencing interpersonal relationships, the structure of the labor market, and forms of cultural participation. In light of the concept of technological determinism, it can be argued that technology is the fundamental driving force behind social, cultural, and economic change. Technological development is inevitable, and its impact on various spheres of human life is becoming increasingly intense and comprehensive[1]. As a result, we are witnessing a gradual transformation of traditional behavior patterns and values, as well as the emergence of new challenges related to digitization, automation, and the rapid development of artificial intelligence.

[1] K. Mania, Deepfake: nowe narzędzie dezinformacji we współczesnej fotografii, „Com.press" 2024, no. 7(2), p. 27.

The beginnings of research into artificial intelligence date back to the 1950s, when British mathematician and computer scientist Alan Turing published an article entitled Computing Machinery and Intelligence, in which he presented the concept of the so-called Turing test, designed to assess the ability of machines to exhibit intelligent behavior[2].

The concept of artificial intelligence is now widely used around the world and covers a diverse range of topics, from machine learning, through neural networks and cognitive computing, to natural language processing. A key element of artificial intelligence is the ability of computer systems to automatically learn from patterns, functions, or data, enabling them to adapt and improve themselves in the process of performing tasks. It is precisely this ability to learn that makes software "intelligent," as it can not only process information, but also draw conclusions and improve its performance in response to problems encountered[3]. As a result, all technologies based on artificial intelligence are becoming an integral part of social life, influencing the way individuals act, communicate, and participate in social structures.

The dynamic development of artificial intelligence in recent years has significantly revolutionized social reality, gaining increasing importance in various areas of social life. In the course of continuous technological improvement, one of the most significant innovations is currently considered to be the phenomenon of deepfakes, which plays an important role especially in the areas of media, communication, and politics. Advances in artificial intelligence, particularly in the field of advanced machine learning techniques and neural networks, have enabled the creation of so-called deepfakes – digital visual and audio content that imitates reality in an extremely realistic way[4]. This phenomenon is a direct result of AI systems' ability to analyze and reproduce patterns based on data, which allows them to create content that is difficult to distinguish from authentic content, while at the same time posing significant socio-cultural challenges related to the verification of information accuracy and trust in digital media, especially in the context of today's world dominated by the Internet and social media as the main sources of information[5].

The article discusses deepfakes as a tool for digital manipulation and disinformation. The aim of the article is to present the essence of the deepfake phenomenon, analyze the mechanisms of manipulation and disinformation in the context of deepfakes, and discuss measures to counteract the deepfake phenomenon, with particular emphasis on regulatory strategies and methods of limiting the negative effects of this technology in the digital space.

[2] K. Pięta, ChatGPT w edukacji – szanse i zagrożenia, „Roczniki Nauk Społecznych" 2024, vol. 16(52), no. 2, p. 151.

[3] K. Paisley, E. Sussman, Artificial Intelligence Challenges and Opportunities for International Arbitration „NYSBA New York Dispute Resolution Lawyer" 2018, vol. 11, no. 1, p. 36, https://sussmanadr.com/wp-content/uploads/2018/12/artificial-intelligence-in-arbitration-NYSBA-spring-2018-Sussman.pdf, [access: 24.10.2025].

[4] N. Young, DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, New York 2019, p. 14.

[5] O. Wasiuta, Sieci społecznościowe jako nowe narzędzia prowadzenia wojen informacyjnych we współczesnym świecie, [in:] O. Wasiuta (ed.), Refleksje o przeszłości, spojrzenie na współczesność: monografia poświęcona Profesorowi Sergiuszowi Wasiucie z okazji 60-letniego Jubileuszu i 35-lecia pracy zawodowej, Kraków 2018, pp. 184-209.

The essence of the deepfake phenomen

The concept of deepfake is a relatively new phenomenon described in scientific literature[6], which is currently spreading rapidly and gaining importance in the context of contemporary digital media. Deepfake technology emerged at the turn of the second decade of the 21st century as a result of the dynamic development of artificial intelligence. The origins of the deepfake phenomenon can be traced back to the Reddit internet forum, where in 2017 a user with the nickname "deepfakes" published fabricated pornographic material featuring, among others, actress Gal Gadot. Using modern software, the video was modified in such a way that the woman's face was placed in existing pornographic scenes. This incident sparked a new and disturbing trend on the internet – since then, fake content featuring images of public figures has been appearing more and more often, used both for satirical purposes and to discredit individuals or promote certain ideas[7].

The name "deepfake" comes from a combination of the words deep learning and fake, meaning "false, insincere." This technology uses advanced machine learning algorithms to manipulate and generate multimedia content that is difficult to distinguish from the real thing with the naked eye[8]. The term deepfake is defined as a technology for imaging people that uses artificial intelligence to alter images of humans[9] or an artificial intelligence-based solution that enables the creation of realistic images, videos, and sounds, although it should be emphasized that these creations are not real, but entirely computer-generated[10], where the main purpose of deepfakes is to generate highly realistic visual and audio content which, despite its apparent authenticity, does not reflect the actual state of affairs.

Deepfake technology is the result of advances in artificial intelligence and is based on deep learning techniques, in which GAN (Generative Adversarial Networks) neural networks play a key role. These networks operate on the basis of two interdependent structures: a generator and a discriminator. The generator is responsible for creating fake images, videos, or sounds, trying to imitate real data as closely as possible. The discriminator, on the other hand, evaluates the generated material, distinguishing between that coming from the generator and authentic data. The feedback provided by the discriminator allows the generator to gradually improve its performance, increasing the realism of the content it creates[11]. The mechanism behind deepfakes shows how modern artificial intelligence enables the generation of highly credible content, while creating new challenges in terms of information verification.

In the digital space, four main categories of deepfakes are most commonly distinguished: entertainment – playful in nature. They often refer to pop culture, and the characters are usually celebrities, actors, anonymous and fictional people;

---

[6] O. Wasiuta, S. Wasiuta, Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość, „Studia de Securitate" 2019, no. 9(3), p. 20.

[7] I. Dąbrowska, Deepfake – nowy wymiar internetowej manipulacji, „Zarządzanie Mediami" 2020, vol. 8(2), p. 91.

[8] A. M. Almars, Deepfakes Detection Techniques Using Deep Learning: A Survey, „Journal of Computers and Communications" 2021, vol. 09(05), p. 28.

[9] I. Dąbrowska, op.cit., p. 90.

[10] O. Rajtar, Technologie deepfake w zakresie danych osobowych, „Rocznik Administracji Publicznej" 2025, no. 1(11), p. 194.

[11] I. Okulska, Sieci neuronowe typu GAN i GPT-2, słowa zużyte i kreatywność, czyli literacki second-hand, „Forum Poetycki" 2019, no. 18, p. 27-28, http://fp.amu.edu.pl/wp-content/uploads/2020/03/InezOkulska_SieciNeuronoweGANiGPT2_ForumPoetyki_18_2019.pdf, [access: 27.10.2025].

educational – aimed at educating the audience. Often using images of famous people, including those who are deceased; discrediting – aimed at weakening the position of a given person, group, organization, or brand. Politicians are most often the target of this type of deepfake; disinformation – causes misinformation, media hype, and social unrest. This applies to both public and private individuals[12]. It is worth noting that this technology is used not only in the above-mentioned categories, but also in less conventional areas – in advertising, film, computer games, digital art, and the creation of virtual avatars. Positive applications include, for example, historical reconstructions, educational materials for people with disabilities, and innovative ways of presenting information in the digital space.

The scale of deepfakes spreading online is growing extremely rapidly. In 2023, approximately 95,820 deepfake videos were recorded, which represents a 550% increase compared to 2019[13]. In 2023, this number rose to approximately 500,000 deepfake video and audio materials shared on social media[14]. Forecasts indicate that by the end of 2025, this number could reach as many as 8 million materials[15]. This growth is the result of the widespread use of artificial intelligence-based tools that enable the creation of realistic video and audio content. The tools do not require any special programming skills or STEM competencies[16]. This means that anyone with access to a computer and the Internet can generate images, text, or videos that are strikingly similar to authentic ones. Such actions, based on the human eye-centered perception of truth, can easily mislead individuals and, through the rapid dissemination of information via social media, reach a significant number of recipients[17] and, as a consequence, lead to manipulation and misinformation of recipients. For this reason, it seems necessary to take a closer look at the mechanisms of manipulation and misinformation that use deepfakes in the modern digital environment.

Manipulation and disinformation mechanism in the context of deepfakes

The digital age, dominated by the Internet and social media, has transformed the world into a space susceptible to manipulation and falsification of

[12] I. Dąbrowska, op.cit., p. 96.
[13] 2023 State Of Deepfakes: Realities, Threats, and Impact, 2023, https://www.securityhero.io/state-of-deepfakes/?utm_source=chatgpt.com, [access: 24.10.2025].
[14] A. Romanishyn, O. Malytska, V. Goncharuk, AI-driven disinformation: policy recommendations for democratic resilience, „Front Artif Intell" 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12351547/?utm_source=chatgpt.com, [access: 24.20.2025].
[15] S. Ramiez, R. A. Lee, Deepfake Statistics 2025: The Hidden Cyber Threat, 2025, https://sqmagazine.co.uk/deepfake-statistics/?utm_source=chatgpt.com, [access: 24.10.2025].
[16] The acronym STEM (Science, Technology, Engineering, and Mathematics) is a term used to group academic disciplines. The term is mainly used in relation to education policy in order to improve competitiveness in the field of science and technology development. STEM education aims to develop analytical skills, critical thinking, problem solving, and teamwork in pupils and students, which are key in today's knowledge- and technology-based world.
[17] E. Sadowska, Ewolucja Cyberzagrożeń: Deepfake i Media Syntetyczne w kontekście bezpieczeństwa energetycznego Europy Wschodniej, „Studia Wschodnioeuropejskie" 2023, expert no. 19-t (2), p. 9.

information. On the Internet, recipients are increasingly faced with an overload of information and are constantly making selections, as they are exposed to the risk of receiving false news[18]. The constant flow of content, generated by both professional media and individual users, blurs the line between reliable and false information. As a result, there is a growing risk of accepting and further disseminating false information, which contributes to the emergence of phenomena such as fake news, understood as media messages that are neither true nor false, are based on misinformation, and often contain fragments of truth[19]. Today, this phenomenon has developed into the increasingly popular form of deepfakes. As a result, the information space has become a battleground for the audience's attention, where truth is increasingly giving way to emotions, sensationalism, and algorithmically amplified content.

Manipulation is generally perceived as an undesirable social influence[20], includes deliberate procedures and mechanisms that enable the control of the thoughts, emotions, and behaviors of other people who are not fully or partially aware of this fact[21]. Currently, it is the Internet that provides the ideal space for manipulating social actors in the context of social, economic, cultural, and political aspects[22] because it enables the rapid dissemination of information, often without verification of its accuracy, which allows it to influence the opinions, attitudes, and decisions not only of individuals but also of entire social groups. On the other hand, online disinformation is often a direct result of manipulation, perceived as a form of false or misleading information that is created with the intention of misinforming or confusing the recipient. The purpose of disinformation is to create confusion, promote a specific outcome, or gain financial or political advantage[23]. In the digital environment, manipulation and disinformation have taken on a new dimension, primarily due to the specific nature of the Internet and social media, which introduce several important factors such as: the speed and reach of information, ease of publication and low barriers to entry, content selection algorithms, the difficulty of verifying information, the “information bubble” effect and polarization, and new manipulative technologies, including deepfakes.

In the context of deepfake technology, the following mechanisms are particularly important for manipulating and misinforming Internet users:

- Interference with people's image and identity – an example is the falsification of the faces of well-known figures, such as politicians or celebrities, in order to attribute words or actions to them that they did not actually say or do. Equally important is the creation of synthetic video and audio recordings that aim to evoke specific emotions in viewers and shape public opinion by presenting a manipulated version of reality;
- Political and social disinformation – involves the use of deepfakes to spread false information during election campaigns, protests, or social conflicts, as well as the creation of materials aimed at undermining the credibility of public figures or institutions;

[18] O. Wasiuta, S. Wasiuta, op.cit., p. 19.
[19] K. Bąkowicz, Wprowadzenie do definicji i klasyfikacji zjawiska fake news, „Studia Medioznawcze” 2019, vol. 20, no. 3(78), p. 281.
[20] M. Antosik, Człowiek współczesny w obliczu manipulacji, „Warmińsko-Mazurski Kwartalnik Naukowy, Nauki Społeczne” 2014, no. 1, p. 41.
[21] H. Hamer, Psychologia społeczna. Teoria i praktyka, Warszawa 2005, p. 211.
[22] K. Pięta, Dezinformacja jako narzędzie manipulacji w sieci, „dot.pl” 2024, no. 1, p. 6.
[23] K. Materska, Informacja w organizacjach społeczeństwa wiedzy, Warszawa 2007, p. 23-26.

- Manipulation of audience emotions – involves reinforcing the message through the use of emotional images and tone of voice, which increases the credibility of false content, and creating materials designed to evoke fear, anger, or sympathy in order to shape public sentiment and influence audience opinions;
- Media and propaganda disinformation – the production of fake news in the form of realistic video recordings enables their publication on social media, while deepfake technologies are used by states or interest groups in propaganda activities, increasing the reach and effectiveness of information manipulation;
- Commercial and image manipulation – includes creating fake advertisements, opinions, or recommendations using the image of famous people and impersonating experts, influencers, or brands for financial gain;
- Cyberbullying and blackmail – referred to as deepfake blackmail, which involves generating compromising material in order to coerce certain actions, ridicule victims, or disseminate false intimate content, known as deepfake pornography[24];
- Perceptual and cognitive manipulation – blurs the lines between reality and fiction, leading to a loss of trust in the media and institutions, and causing the so-called “doubt effect,” in which even true materials may be questioned as potential manipulations.

It should be emphasized that all deepfake content is constructed according to carefully designed marketing and propaganda schemes that repeatedly use specific persuasive blocks. They include an introduction in the form of an emotional story or a supposedly spontaneous statement, a description of the problem presenting a threatening situation, arousing the viewer's emotions through fear, anger, or frustration, appealing to authority, presenting a “solution” in the form of a product, service, or investment, false evidence of effectiveness, and a call for immediate action. The effectiveness of manipulation is increased by tailoring the language and style of the message to the target audience – from colloquial and youth language in social media, through expert language, to lofty, political, or preachy forms aimed at older people. This content includes direct appeals to the audience, references to national identity and “real life” and the form often imitates popular media formats, which lowers the audience's vigilance. In addition, they use fake reviews, comments, or expert recommendations, conspiracy narratives, and “truth revealed” theories. They often take the form of emotional swings, leading the recipient from fear and a sense of betrayal to swift action, which not only encourages interaction but can also escalate aggression and incite immediate, impulsive reactions[25].

The above analysis shows that with the rapid development of deepfake technology, its importance as a tool for manipulation and disinformation is growing, while at the same time the spectrum of online threats is expanding significantly, enabling sophisticated and multidimensional forms of influence. The impact of these technologies extends beyond the image and emotions of the audience to social, political, and commercial relations, as well as the perception of reality,

[24] Deepfakes, Police.uk, https://www.police.uk/advice/advice-and-information/online-safetyonline-safety/deepfakes-what-is-a-deepfake/?utm_source=chatgpt.com, [access: 28.10.2025].

[25] Portal sztucznej inteligencji, Techniki manipulacji w świecie deepfake’ów – jak sztuczna inteligencja zmienia oblicze dezinformacji, https://www.gov.pl/web/ai/techniki-manipulacji-w-swiecie-deepfakeow-jak-sztuczna-inteligencja-zmienia-oblicze-dezinformacji, [access: 28.10. 2025].

making them a significant challenge to information security and public trust. It therefore seems important to focus on strategies to combat deepfakes in the digital space in order to limit their negative impact, increase the audience's resistance to manipulation and disinformation, and support reliable and secure online communication.

Strategies for combating deepfakes in the digital space

In view of the rapid development of deepfake technology and the growing influence of manipulated content on public opinion, it is extremely important to develop effective strategies to counteract its negative effects. The fight against deepfakes requires a multidimensional approach, combining legal, technological, and educational measures that allow for both the detection and verification of manipulated materials and the raising of public awareness about disinformation. An important step in counteracting the negative effects of deepfake technology is the implementation of appropriate legal regulations that precisely define the scope of responsibility of persons involved in the creation, publication, and dissemination of manipulated digital content. These regulations should include sanctions for illegal activities, including fraud, blackmail, disinformation, and the deliberate destruction of the reputation of both private and public figures. In response to the growing threats associated with the use of artificial intelligence-based technologies, including deepfakes, the institutions of the European Union—particularly the European Commission as the initiator and the European Parliament and the Council as co-legislators developed two key pieces of legislation: the Digital Services Act (DSA)[26] and Artificial Intelligence Act (AI Act)[27]. These documents impose an obligation on large online platforms to identify, label, and limit the dissemination of manipulated content, and introduce requirements for transparency and ethical use of artificial intelligence solutions. The aim of these regulations is to create a safer and more reliable digital space where users can consciously assess the authenticity of the information available[28].

Unfortunately, implementing legal regulations to combat the misuse of deepfake technology is a complex and lengthy process that requires close cooperation between countries, EU institutions, and the technology sector. Currently, EU member states are facing numerous difficulties in adapting existing regulations to the rapidly changing technological reality. These challenges concern not only differences in the implementation of regulations at the national level and in the effectiveness of detecting synthetic content, but also the lack of appropriate technological tools enabling the identification of manipulated materials in real time[29], which consequently causes deepfakes to spread faster than digital platforms can detect and flag them as AI-generated content.

[26] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending 2000/31/EC (Digital Service Act), OJ L 277, 27.10.2022, p.1-102, http://data.europa.eu/eli/reg/2022/2065/oj, [access: 31.10.2025].
[27] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 1689, 12.02.2024, http://data.europa/eu/eli/reg/2024/1689/oj, [access: 31.10.2025].
[28] NASK, Deepfaki - prawdziwy problem z fałszywą rzeczywistością, https://www.nask.pl/magazyn/deepfaki-prawdziwy-problem-z-falszywa-rzeczywistoscia, [access: 31.10.2025].
[29] Ibidem.

Contemporary information societies today face the dilemma of how to effectively counteract the negative effects of the dynamic development of generative technologies without violating fundamental democratic values.

Technological methods used to combat deepfakes, such as: deepfake detection tools, the use of “digital signature” mechanisms or watermarking in digital media, the use of blockchain technology or similar solutions to ensure a permanent and auditable chain of origin for digital materials, or the use of stronger authorization and identity verification in digital communications, e.g., biometric verification systems, multi-factor authentication (MFA), may be insufficient as they are only part of an effective strategy to combat deepfakes. To be effective, they must be complemented by educational, regulatory, and ethical measures that together form an integrated system of protection against digital manipulation. Furthermore, it should be remembered that, on the one hand, legal regulations and all possible strategies for combating deepfakes should protect users from disinformation and manipulation, while on the other hand, they must not violate the fundamental principle of freedom of speech. Consequently, combating deepfakes is a multidimensional challenge, involving not only technological issues, but also ethical and political ones, requiring a balanced approach and international cooperation[30].

Considering the strategies for counteracting deepfakes presented above, it should be emphasized that effectively combating this problem requires not only technological and legal solutions, but also, above all, coordinated actions in the field of social education and raising the awareness of content consumers about the potential threats resulting from the development of synthetic media and generative technologies. Building a culture of skepticism towards unverified digital information, implementing procedures within organizations, e.g., at work, or training and information campaigns for the public can help increase users' information resilience and limit the effectiveness of manipulation and disinformation generated using deepfake technology.

Summary

In summary, the above theoretical analysis allows us to conclude that deepfake technology is currently a complex phenomenon, combining both enormous development potential and significant social and ethical risks. On the one hand, deepfake technology is used in many areas of social life, enabling the creation of realistic simulations, historical reconstructions, and personalized teaching materials. On the other hand, however, the development of this technology leads to a constant increase in the problem of disinformation, manipulation of public opinion, and violations of the image and privacy of individuals, which in turn requires comprehensive measures to be taken to limit the negative effects of its use and ensure the responsible and safe use of deepfakes in the public sphere.

From a legal perspective, it seems necessary to introduce and effectively enforce regulations that will protect not only individuals but also institutions from the harmful use of deepfake technology. The law should provide for penalties for the creation and dissemination of manipulated material for criminal purposes, and introduce an obligation to clearly label content generated by artificial intelligence, which would undoubtedly contribute to increasing the transparency of media

[30] Ibidem.

messages, strengthening public trust in information published on the internet, and limiting the effects of disinformation and manipulation.

It is worth emphasizing that effective counteraction against the negative effects of deepfake technology also requires broad cooperation between various sectors. Joint action by the public sector, the private sector, the media sector, scientific and academic circles, and non-governmental organizations seems crucial and necessary to limit the phenomenon of manipulation and disinformation in the public sphere. Only by combining efforts in these areas is it possible to realistically minimize the risk of abuse and ensure greater credibility and integrity of information, while supporting communities in building resilience to manipulation and disinformation.

Literature

Almars A. M., Deepfakes Detection Techniques Using Deep Learning: A Survey, „Journal of Computer and Communications" 2021, vol. 09(05), DOI: https://10.4236/jcc.2021.95003.

Antosik M., Człowiek współczesny w obliczu manipulacji, „Warmińsko-Mazurski Kwartalnik Naukowy, Nauki Społeczne" 2014, no. 1.

Bąkowicz K., Wprowadzenie do definicji i klasyfikacji zjawiska fake news, „Studia Medioznawcze" 2019,vol. 20, no. 3(78).

Dąbrowska I., Deepfake – nowy wymiar internetowej manipulacji, „Zarządzanie Mediami" 2020, vol. 8(2), DOI: https://doi.org/10.4467/23540214ZM.20.024.11803.

Hamer H., Psychologia społeczna. Teoria i praktyka, Warszawa 2005.

Mania K., Deepfake: nowe narzędzie dezinformacji we współczesnej fotografii, „Com.press" 2024, no. 7(2), DOI: https://doi.org/10.33077/uw.24511617.ms.2019.2.106.

Materska K., Informacja w organizacjach społeczeństwa wiedzy, Warszawa 2007.

NASK, Deepfaki - prawdziwy problem z fałszywą rzeczywistością, https://www.nask.pl/magazyn/deepfaki-prawdziwy-problem-z-falszywarzeczywistoscia.

Okulska I., Sieci neuronowe typu GAN i GPT-2, słowa zużyte i kreatywność, czyli literacki second-hand, „Forum Poetyki" 2019, no. 18.

Paisley K., Sussman E., Artificial Intelligence Challenges and Opportunities for International Arbitration, „NYSBA New York Dispute Resolution Lawyer" 2018, vol. 11, no. 1, https://sussmanadr.com/wp-content/uploads/2018/12/artificial-intelligence-in-arbitrationNYSBAspring2018Sussman.pdf.

Pięta K., ChatGPT w edukacji – szanse i zagrożenia, „Roczniki Nauk Społecznych" 2024, vol. 16(52), no. 2, DOI: https://doi.org/10.18290/rns2024.0024.

Pięta K., Dezinformacja jako narzędzie manipulacji w sieci, „dot.pl" 2024, no. 1, DOI: https://doi.org/10.60097/DOTPL/196011.

Rajtar O., Technologie deepfake w zakresie danych osobowych, „Rocznik Administracji Publicznej" 2025, no. 1(11), DOI: https://doi.org/10.4467/24 497800RAP.25.011.21303.

Ramiez S., Lee R. A., Deepfake Statistics 2025: The Hidden Cyber Threat, 2025, https://sqmagazine.co.uk/deepfake-statistics/?utm_source=chatgpt.com.

Sadowska E., Ewolucja Cyberzagrożeń: Deepfake i Media Syntetyczne w kontekście bezpieczeństwa energetycznego Europy Wschodniej, „Studia Wschodnioeuropejskie" 2023, expert no. 19-t (2), DOI: 10.31971/24500267.20.15.

Wasiuta O, Sieci społecznościowe jako nowe narzędzia prowadzenia wojen informacyjnych we współczesnym świecie, [in:] O. Wasiuta (ed.), Refleksje o przeszłości, spojrzenie na współczesność: monografia poświęcona Profesorowi Sergiuszowi Wasiucie z okazji 60-letniego Jubileuszu i 35-lecia pracy zawodowej, Kraków 2018.

Wasiuta O., Wasiuta S., Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość, „Studia de Securitate" 2019, no. 9(3), DOI: https://doi.org/10.24917/26578549.9.3.2.

Young N., DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, New York 2019.