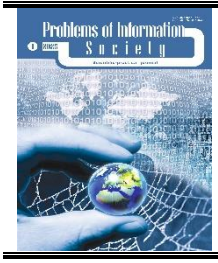

www.jpis.az

Cybersecurity issues in journalism based on artificial intelligence technologies

Sunbul Zalova

Institute of Information Technology, Baku State University, Baku, Azerbaijan

sunbulzalova@gmail.com

https://orcid.org/0000-0002-5598-7266

ARTICLE INFO

http://doi.org/10.25045/jpis.v16.i1.11

Article history:
Received 12 August 2024
Received in revised form
15 October 2024
Accepted 21 January 2025

Keywords:

Artificial intelligence technologies
Cybersecurity
Journalism
Digital media
Disinformation
Digital media content

ABSTRACT

Although the use of artificial intelligence in journalism creates innovations and opportunities, this process leads to complications in a number of cybersecurity issues. One of the main problems is the risk of disinformation and manipulation. Although artificial intelligence algorithms automatically process information, it is possible for these algorithms to make decisions based on incorrect information, which can result in the dissemination of biased or false news. At the same time, the database used in artificial intelligence programming can affect its objectivity and impartiality. The use of data collected by artificial intelligence and sources without verification can lead to the dissemination of untrustworthy and inaccurate news. This article examines cybersecurity issues arising from the application of artificial intelligence technologies in journalism. Artificial intelligence technologies are currently widely used at all stages of news production. It highlights the current situation regarding artificial intelligence technologies and the application of these technologies to journalism, as well as the problems encountered in this field. This article examines the problems arising from the application of artificial intelligence technologies. "Deepfake" technologies, their negative aspects, and the problems they may cause are studied. Proposals are made for solving cybersecurity issues and a conceptual model is developed.

1. Introduction

Artificial intelligence (AI) journalism is a field that combines the power of AI with the principles and values of journalism. AI in journalism has the potential to revolutionize this field by automating certain tasks such as data analysis and fact-checking, and by increasing the speed and efficiency of news production. To ensure the integrity and credibility of news, ethical considerations should be at the forefront of AI journalism (Kim et al., 2019).

The use of AI in journalism can lead to more accurate and reliable news coverage, but it is important to maintain ethical standards throughout the process. This requires transparency in the use of AI algorithms, ensuring that they are unbiased and do not promote any particular agenda.

The use of AI in journalism creates a deep connection between technology and journalism. This leads to "hacking" attacks, data theft or manipulation of both AI and the systems on which journalists work. These problems include the risk of disinformation, the spread of biased information, the reliability of sources, etc.

AI has led to significant advances in journalism in recent years. Various news agencies, newspapers and online media platforms are using AI technology to collect information, analyze it and even create news (Dörr et al., 2016). However,

the application of AI in journalism also raises a number of cybersecurity issues. This article examines the problems created by the use of AI in journalism and offers solutions.

It is important for journalists and media organizations to take cybersecurity seriously. AI can easily affect and manipulate people. Therefore, it is necessary to be careful when using AI and identify the biases of algorithms, consequently, AI tools cannot be completely trusted (Indora et al., 2024). The article examines in detail the cybersecurity issues created by AI technologies in journalism.

2. Related works

AI has begun to be widely used in journalism, especially in leading news organizations. Despite the numerous advantages that AI brings to journalism, a number of problems prevent its expansion and spread among journalists. The problems created by AI systems in terms of cybersecurity concern journalists. One of the problems that AI technologies pose in journalism is related to ethical rules. A study was conducted in Jordan to investigate the ethical problems posed by the application of AI in journalism. In-depth interviews were conducted with 14 journalists working in the newsroom of the state-owned "Al Mamlaka" TV. The information obtained from the interviews was analyzed thematically. The studies showed that the main ethical problems that journalists face in newsrooms related to the application of AI included data bias, violation of confidentiality, and the lack of legislation and international rules regarding the use of AI in journalism (Abdullah et al.,2024).

Many scientific articles, books, and research studies related to the problems arising from the application of AI technologies in journalism are available nowadays (Sharp et al., 2023; Buyers et al., 2023; Stamp et al., 2022).

(Sharp et al., 2023) examines cybersecurity in the era of AI, how to stay safe in the digital world, this powerful intersection of technologies, and how it is changing our understanding of digital security. The study simplifies highly technical information into understandable concepts, providing a comprehensive and in-depth examination of the role of AI in protecting our data and digital footprints from growing threats for a broad audience.

Another study outlines the fundamentals that distinguish AI systems from traditional technologies and explains the differences between AI, machine learning, deep learning, and generative AI (and additional key models). This study explains that the application of AI technology poses challenges and risks that need to be carefully considered, including the importance of causality, intellectual property ownership, privacy, and data protection. The study also provides a detailed discussion of AI ethics and the new AI Act (Buyers et al.,2023).

(Stamp et al., 2022). examines new and emerging applications of machine learning, deep learning, and AI that pose significant cybersecurity challenges. The presented research goes beyond simply applying AI techniques to datasets and instead explores deeper issues at the intersection of deep learning and cybersecurity. The research paper provides insight into the complex "how" and "why" questions that arise when using AI in security. For example, this research includes research on "explainable AI", "healthy AI" and a wide range of related topics.

This research paper aims to explore the role of AI in journalism and the underlying causes of cybersecurity problems that arise in this regard, and to present strategies for solving them.

Problem statement. The paper examines the problems arising from the application of AI technologies, examines "Deepfake" technologies, their negative aspects, the problems they may cause, provides suggestions for solving cybersecurity issues, and develops a conceptual model.

3. Materials and Methods

3.1. Cybersecurity issues in AI-based journalism

The application of AI technologies in journalism has raised a number of cybersecurity issues. Fig. 1 illustrates cybersecurity issues in AI-based journalism.

Several official documents and laws have been adopted to address the challenges posed by the application of AI technologies to journalism. One of them is the European Union Artificial Intelligence Act (EU AI Act, 2023). This law creates a common regulatory and normative framework for AI within the EU (Shaping Europe's digital future, 2021). The draft law, proposed by the European Commission on 21 April 2021, was read in the European Parliament on 13 March 2024 and unanimously approved by the EU Council on 21 May 2024 (Mackrael et al., 2024.)

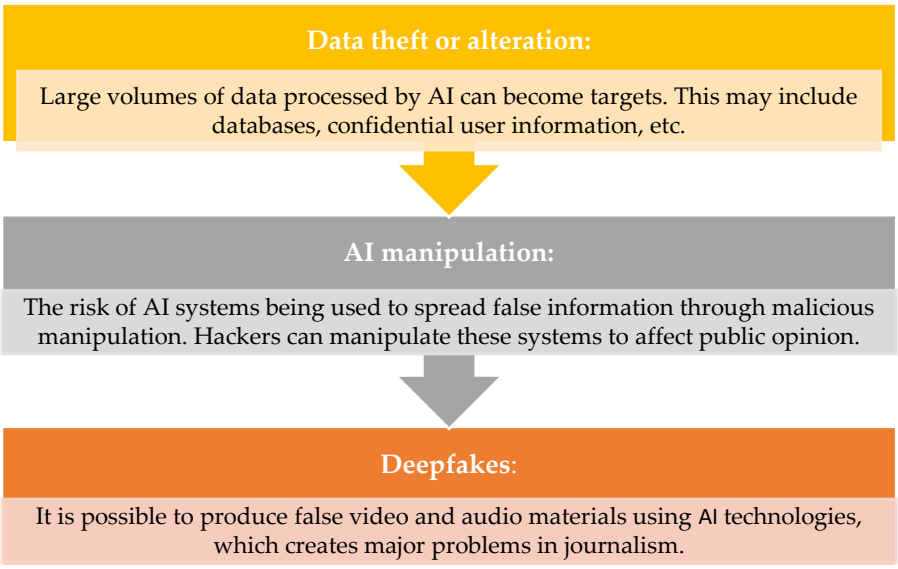

Fig. 1. Cybersecurity issues in AI-based journalism

The law also provides for the establishment of a European Council on AI to promote national cooperation and ensure compliance with the regulation (Gilchrist et al., 2024). The main objective of this law is to ensure the safe and secure use of AI technologies in EU. The AI Act focuses particularly on regulating high-risk technologies, increasing transparency and protecting human rights. At the same time, the draft law ensures the safe use of these technologies through regulation, without hindering the development of technological innovation. The adoption of the Act in 2023 was implemented after negotiations between the EU Council and the European Parliament, and the implementation mechanisms and control structures were stated to be formed in the next stages for the law to enter into full force.

The AI Act is the first comprehensive bill regulating the safe and ethical use of AI technologies in the EU. Proposed in 2021, this bill aims to minimize the risks of the technologies and provide a legal framework, given the widespread use of AI in society. The act aims to create a single European-wide framework for the proper regulation of high-risk AI systems specifically. The main objective of the AI Act is to ensure the use of AI within cybersecurity and ethical frameworks, as well as to minimize the potential harm of these technologies. This bill ensures that the threats that AI can pose to society and individuals are managed without hindering the development of technological innovation in Europe.

Table 1 presents the cybersecurity challenges posed by AI technologies in journalism

Table 1. Problems posed by AI technologies in journalism

Impartiality and Objectivity	One of the main principles of journalism is objectivity. AI systems make decisions based on the data and algorithms they are programmed to use. These algorithms can represent the biases and approaches of their creators. For example, AI can provide biased information on a particular political or social topic because it is based only on specific databases or models.
Reliability and Use of Sources	The processing of large volumes of data by AI allows journalists to use a vast database. However, this can result in a lack of attention to the reliability of sources. Information collected by AI can be published without checking the accuracy and reliability of the sources, which is contrary to the ethical rules of journalism.
Determination of Responsibility	The issue of liability for content generated by AI is being debated. If a story is automatically generated by AI and turns out to be false, who is responsible? The answer to this question is not yet entirely clear, as there are no clear rules on the legal status and liability of AI. Journalists and news agencies should be more transparent in their use of AI and take responsibility for the information generated by this technology.

Protection of Personal Data	As AI facilitates the processing of large amounts of data, the issue of privacy is also on the agenda. Although much of the data analyzed by AI is obtained from public sources, in some cases, the improper protection of personal data can lead to ethical and legal problems. Therefore, journalists must ensure that AI applications respect data privacy.
Transparency and accountability	The use of artificial intelligence in journalism should be publicized and transparent. Content created using AI should be openly labeled and journalists should provide clear explanations of how these technologies work.

The application of AI technologies in journalism can create several cybersecurity problems. The basic principles of journalism: accuracy, objectivity and responsibility should be preserved even when using AI. The main cybersecurity issues arising in AI journalism are as follows:

Risk of disinformation and manipulation. Content creation through AI increases the speed of data processing and minimizes human errors. However, excessive automation of AI can lead to the spread of disinformation. For example, it is possible for false information to be accidentally or deliberately inserted into news content by AI. This can lead to the widespread dissemination of biased information and the manipulation of public opinion. AI technologies, especially when used for automatic processing and dissemination of data, can facilitate the rapid spread of false or misleading information.

This is especially relevant with the use of technologies such as "deepfakes". Fake images, videos, and news stories generated by AI can undermine public trust. A key challenge for journalists and media outlets is to verify the authenticity of information generated by AI and prevent false information.

New digital technologies are making it increasingly difficult to distinguish between real and fake media. Combined with the reach and speed of social media, false information can quickly reach millions of people.

"Deepfakes" are technologies that use AI to create fake images and videos that mimic the facial expressions, voices, and movements of people with the appearance or speech style of another person (Westerlund et al., 2019) "Deepfakes" are mainly used to replace people's faces or voices in videos.

- Face swapping: The facial expressions and movements of one person can be transferred to the face of another person.
- Voice imitation: AI can imitate the voice of a person and fake a conversation on their behalf.

Deepfakes technologies are based on the following main components of AI:

Generative Adversarial Networks (GANs) refer to a system in which two different AI models work against each other. One model creates fake images, and the other analyzes these images and tries to distinguish between real and fake images. As a result of the competition between these two models, fake and more realistic images are obtained. Deep learning and neural networks - AI technologies analyze a large number of images and videos and learn the facial structures, movements and voice characteristics of individuals. Based on this data, it is possible to create completely new and realistic images.

Fig. 2 presents the advantages of "deepfakes" technology.

The use of "deepfakes" technology can create a number of problems in the field of journalism (Westerlund et al., 2019). Examples may include disinformation and fake news. Fake images and videos can be spread on behalf of political and public figures, which can lead to the spread of misinformation in the public and confusion among people.

"Deepfakes" technology can intrude on privacy, and offensive and harmful content can be created by changing the images and voices of individuals without their consent.

Fake videos and audio recordings created using "deepfakes" technologies can be used as blackmail or threats against people. Various technologies and legal measures should be developed to reduce the threats posed by "deepfakes". New methods are being developed to distinguish fake images from real ones using AI-based tools. These tools try to distinguish between real and fake images by analyzing videos.

AI allows for the automation of journalism, which may lead to the loss of certain areas of activity for journalists. For example, information such as simple news articles or sports scores is already automatically generated by AI.

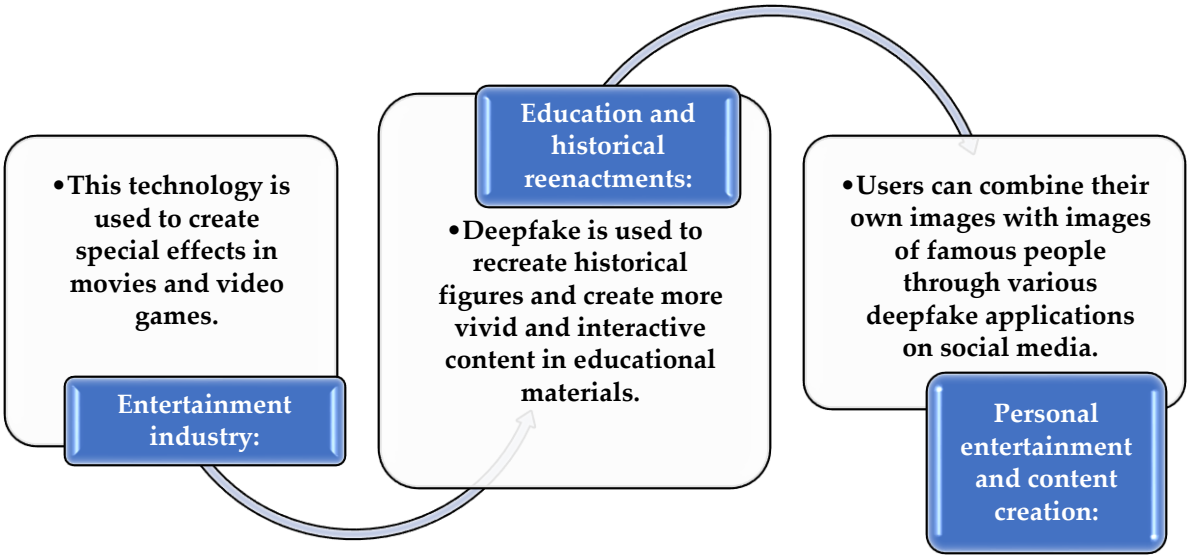

Fig. 2. Advantages of "deepfakes" technologies

This situation raises concerns about the future of professional journalists (Zalova et al., 2024). From an ethical perspective, appropriate measures should be taken to maintain the balance of human labor with the development of technology.

To ensure fair and inclusive news coverage, concerns about bias in algorithms and transparency in AI decision-making processes must be taken seriously (Radsch, 2022). By adhering to ethical principles that uphold transparency, fairness, and the public interest, journalistic organizations can harness the benefits of AI technology while protecting against the persistence of misinformation, discrimination, and harm to marginalized communities. To enhance the social impact of AI in journalism and uphold fundamental journalistic values, it is necessary to foster a culture of ethical awareness among journalists and technologists.

The physical and digital safety of journalists and their sources is under threat in many parts of the world. In particular, digital security and cybersecurity threats are increasingly important for global news media, as journalists and publishers become high-profile targets for digital surveillance, compromising their own and their sources' privacy and security. Digital security and cybersecurity have attracted the attention of policymakers globally, and as of 2021, 156 countries have adopted cybercrime legislation (Journalists & Cyber Threats, 2024).

The article uses empirical research methods. International experience is analyzed. The problems that phishing attacks, data leaks, and social media manipulation can cause are examined.

3.2. Problem Solving

A conceptual model is proposed to systematically understand cybersecurity problems related to the use of AI in journalism and to propose solutions. AI applications can lead to cybersecurity risks, for example, automatic news writing algorithms can facilitate manipulation and disinformation. These risks can be mitigated by implementing security measures against threats, such as data encryption and network protection. Training and ethical guidelines for journalists help to properly manage cybersecurity and the use of AI.

This conceptual model systematically presents cybersecurity problems when using AI in journalism and shows the measures needed to prevent them. It is important to ensure that journalists and editorial offices are informed and prepared on cybersecurity issues.

The conceptual model serves to understand cybersecurity problems related to the use of AI in journalism and to develop strategic approaches to solve them. The interaction between each component allows for more effective steps aimed at increasing security in modern journalism. Fig. 3 illustrated the conceptual model.

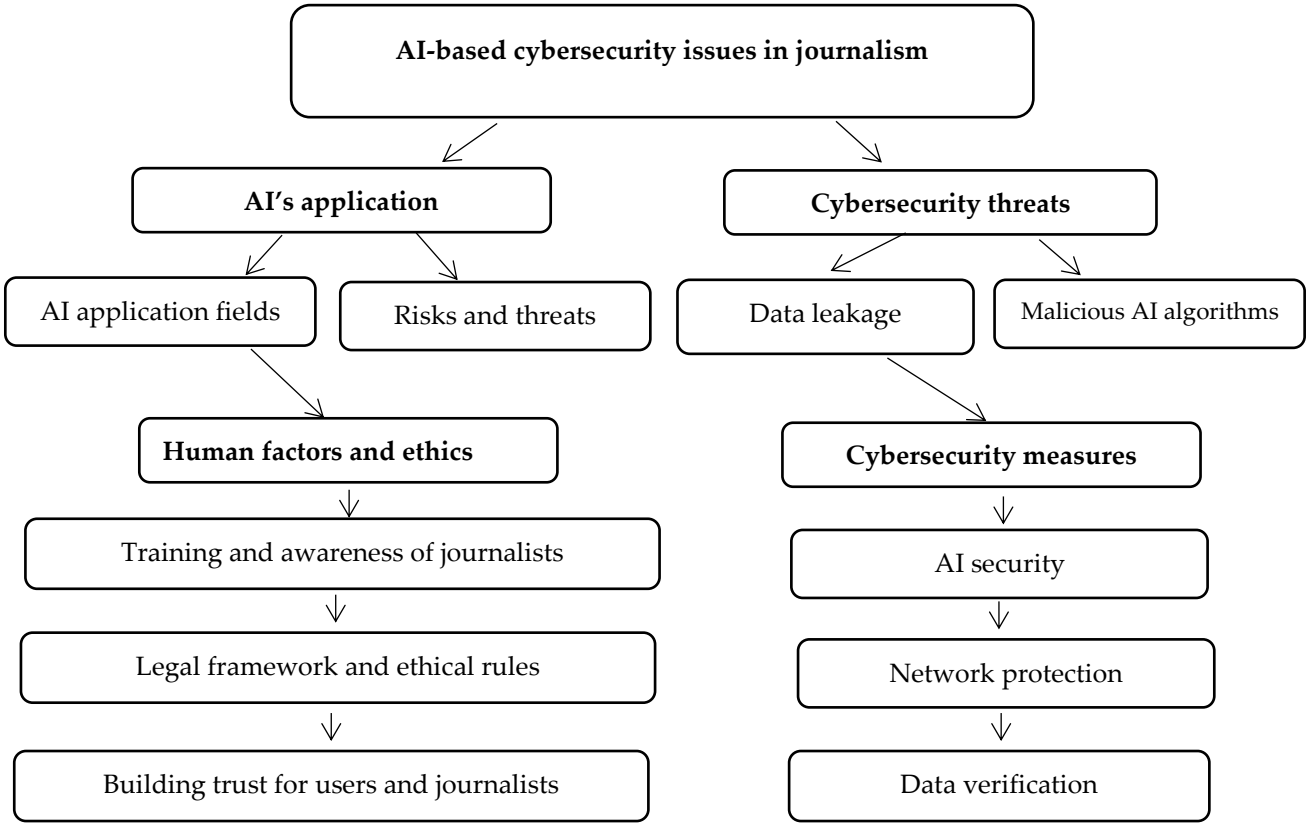

Fig. 3. Conceptual model for cybersecurity problems in AI-based journalism.

4. Discussion

There are various risk categories in the use of AI technologies. Fig. 4 provides detailed information about these risks.

Fig. 4. Risk categories when using AI technologies

This includes, with some exceptions, AI applications that manipulate human behavior, for example, those that use real-time remote biometric identification data (such as facial recognition) in public places, as well as those used for social assessment (evaluating people based on their personal characteristics, socio-economic status or behavior).

High risk - AI applications that are expected to pose serious threats to the health, safety or fundamental rights of people. This category includes, in particular, AI systems used in the fields of healthcare, education, employment, critical infrastructure management, law

Unacceptable risk - AI applications in this category are prohibited, except in special cases (Indora et al., 2024).

enforcement or justice. These applications are subject to quality, transparency, human control and security requirements and, in some cases, are required to undergo a process called a "Fundamental Rights Impact Assessment" before use (Mantelero et al., 2022). They should be assessed both before they are placed on the market and throughout their entire life cycle. The list of high-risk applications can be expanded over time; this does not require changes to the law itself.

General AI risk— This category, included in 2023, includes specific foundational models such as ChatGPT. They are subject to transparency requirements. High-performance general-purpose AI systems (especially those designed to leverage more than 1025 FLOPS of computing power) (Bertuzzi et al., 2023) that may pose systematic risks must also undergo a comprehensive assessment process.

Limited risk — AI systems in this category are subject to transparency requirements, which ensure that users are informed about their interactions with the AI system and allow them to make informed choices. This category includes, for example, AI programs that allow the creation (such as deepfakes) or manipulation of images, sounds, or videos. This category does not regulate open-source (i.e., free models whose parameters are publicly available) except in certain circumstances (Bertuzzi et al., 2023).

Minimal risk — This category includes, for example, AI systems used in video games or spam filters. Most AI applications are likely to fall into this category (Walters et al., 2021). These systems are not regulated and Member States cannot impose additional rules due to the maximum harmonisation rules. The law repeals existing domestic laws on the establishment or use of such systems. However, it is proposed to adopt a voluntary code of conduct (Buyers et al., 2023).

5. Conclusion

The development of regulatory laws is essential to address cybersecurity challenges. The working mechanisms of AI algorithms and decision-making processes must be transparent. No matter how advanced the application of AI in journalism becomes, the complete elimination of human control may lead to ethical problems. Journalists and editors should monitor the content generated or analyzed by AI and verify its objectivity and accuracy. Although AI has great potential in journalism, it is necessary to address the cybersecurity challenges associated with it. To address these challenges, both regulators and media organizations must work together to regulate the application of AI in accordance with ethical and legal norms. Only then effective and beneficial use of AI in journalism can be ensured. The complexity and scale of cybersecurity problems are increasing with the rapid development of technology. Threats such as data leaks, phishing attacks, and malware pose a serious threat to both individual users and large organizations. There is a great need for advanced cybersecurity technologies, including the use of AI, to combat these challenges. However, it is important to strengthen awareness and security policies at both the technical and social levels. Continuous innovation and development of defense strategies should be a top priority to create a secure digital environment. The results of the research indicated that the application of technology to journalism can create new opportunities. Specialists in the field of media and journalism have to adapt to the technological level of social developments. The integration of technology into journalism plays an important role in the formation of an inclusive society. With the help of technology, citizens with disabilities can be provided with information, and can turn to the source of information and make their problem relevant. Furthermore, artificial intelligence technologies can promote the development of inclusive journalism by combating biased information in journalism. It can help to identify ways to solve problems, to investigate whether the solution has a positive or negative result. ICT will be a means of reintegrating people with physical disabilities into society, restoring their independence and becoming equal people in society. The use of artificial intelligence in journalism presents both opportunities and challenges for promoting inclusive media and strengthening social justice. As technology develops, journalists must carefully consider the data they use.

References

Alessandro Mantelero, (2022) Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI, Information Technology and Law Series, 36, The Hague: Springer-T.M.C. doi:10.1007/978-94-6265-531-7, ISBN 978-94-6265-533-1

Bertuzzi, Luca. (2023)."AI Act: EU policymakers nail down rules on AI models, butt heads on law enforcement". https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu policymakers-nail-down-rules-on-ai-models-butt-heads-on-law-enforcement

EU AI Act: first regulation on artificial intelligence (2023). European Parliament News, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Halley Kim (2019). Aİ in Journalism: Creating on Ethical Framework. Syracuse University Honors Program Capstone Projects. 1083. https://surface.syr.edu/honors_capstone/1083

Jacintha Walters, Diptish Dey, Debarati Bhaumik, Sophie Horsman. (2021). Complying with the EU AI Act. Communications in Computer and Information Science Artificial Intelligence, 65-70. https://doi.org/10.1007/978-3-031-50485-3_5

John Sharp. (2023). Cybersecurity in the Age of AI: Staying Safe in the Digital World.

John Buyers (2023) Artificial Intelligence – The Practical Legal Issues (Third Edition).

Journalists & Cyber Threats (2024). Center for News, Technology & Innovation. https://innovating.news/article/journalists-cyber-threats/

Karen Gilchrist, Ruxandra Iordache. (2024) World's first major act to regulate AI passed by European lawmakers, CNBC, https://www.cnbc.com/2024/03/13/european-lawmakers-endorse-worlds-first-major-act-to-regulate-ai.html

Konstantin Nicholas Dörr. (2016) Mapping the field of Algorithmic Journalism. Digital Journalism 4(6): 700–722. DOI: 10.1080/21670811.2015.1096748

Mackrael Kim, Sam Schechner (2024). European Lawmakers Pass AI Act, World's First Comprehensive AI Law. The Wall Street Journal. https://www.wsj.com/tech/ai/ai-act-passes-european-union-law-regulation-e04ec251

Mark Stamp, Corrado Aaron Visaggio, Francesco Mercaldo, Fabio Di Troia (2022). Artificial Intelligence for Cybersecurity (Advances in Information Security, 54).

Mateusz Łabuz (2023). Regulating Deep Fakes in the Artificial Intelligence Act. Applied Cybersecurity & Internet Governance, 1-42. https://doi.org/10.60097/ACIG/162856

Mika Westerlund (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management, 9(11):39-52 https://www.proquest.com/docview/2329154005?sourcetype=Scholarly%20Journals

Omar Abdullah al-Zoubi, Normahfuzah Ahmad (2024). Contemporary tasks for jordanian journalists in the era of artificial intelligence, Arab Media and Society Journal, Issue 37, Winter/Spring https://doi.org/10.70090/ON24CTJJ

Prabhat Indora, Rajeev Singh. (2024). Artificial Intelligence in Journalism: An Overview of its Applications and Uses. Journal of Communication and Management, 237-242, DOI: 10.58966/JCM2024337

Shaping Europe's digital future (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence https://digitalstrategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

Radsch Courtney (2022). Artificial intelligence and disinformation: state-aligned information operations and the distortion of the public sphere, 1-29. https://www.osce.org/files/f/documents/e/b/522166.pdf

Zalova S. (2024). Applying artificial intelligence technologies to inclusive journalism. Problems of Information Society, 15(1):64–71. (in Azerbaijani) http://doi.org/10.25045/jpis.v15.i1.07

Zalova S. (2020) Journalism based on artificial intelligent technologies: problems and prospects. Problems of Information Society, 119–127. (in Azerbaijani) http://doi.org/10.25045/jpis.v11.i1.10