STUDIA IURIDICA TORUNIENSIA
TOM XXXVI
DATA WPŁYWU: 26 LIPCA 2024 R. DATA AKCEPTACJI: 10 GRUDNIA 2024 R.

Krzysztof Kaczmarek
Koszalin University of Technology
krzysztof.kaczmarek@tu.koszalin.pl
ORCID: https://orcid.org/0000-0001-8519-1667

Mirosław Karpiuk
University of Warmia and Mazury, Olsztyn
miroslaw.karpiuk@uwm.edu.pl
ORCID: https://orcid.org/0000-0001-7012-8999

Andrea Spaziani
University of Teramo, Italy
aspaziani@unite.it
ORCID: https://orcid.org/0000-0002-2465-3570

Use of artificial intelligence in public sector: threats and prospects

http://dx.doi.org/10.12775/SIT.2025.002

1. Introduction

In today's highly digitised societies, Information and Communication Technologies (ICT) are present in almost every aspect of modern life, and digital tools are widely used for professional purposes in science and in interpersonal relations.[1] Of all ICTs, the most technologically advanced tool is artificial intelligence (AI).

[1] E.M. Włodyka, *Sztuczna inteligencja w sektorze publicznym – stan i oczekiwania*, in: *Edukacja, komunikacja i dyskursy społeczne. Studia humani-*

Although there is a plethora of scientific literature on artificial intelligence, it is difficult to uniquely define what it is and what it is not.[2] It is a challenging task to determine a given tool as falling into an AI category, and the controversy around defining and understanding the concept of artificial intelligence stems largely from the difficulty in specifying the concept of intelligence itself.[3]

For the purposes of this article, it has been accepted that AI are systems that are capable of performing tasks that were previously only possible through human intelligence, with processes of learning, analysis, and autonomous decision-making occurring much faster than in humans.

The use of AI has a potential to improve and enhance operational efficiency and service quality. This also applies to public services, where the implementation and use of AI is a growing trend.[4] In the public sector, AI can be used in areas such as data management, big data analysis, automation of administrative processes, or in the area of crisis management. At the same time, it can be assumed that algorithms will increasingly be replacing humans in numerous activities. As an example, although current AI tools do not yet allow this, according to experts, the use of AI in public procurement is just a matter of time.[5]

It is also important to bear in mind that, although the potential of AI goes well beyond the capabilities of traditional analytical tools, the technology is constantly evolving and is not flawless.

styczne i społeczne, L.J. Maksymowicz, Z. Danielewicz (eds.), Koszalin 2023, p. 123.

[2] A. Kaplan, M. Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, "Business Horizons" 2019, No. 1, p. 17, https://doi.org/10.1016/j.bushor.2018.08.004.

[3] M. Wójcik, *Sztuczna inteligencja: potencjał dla procesów zarządzania informacją*, "Przegląd Biblioteczny" 2017, No. 1, p. 7.

[4] J. Blicharz, L. Zacharko, *Wdrażanie technologii sztucznej inteligencji w administracji publicznej – kilka refleksji*, in: *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, P. Lisowski (ed.), Wrocław 2024, p. 349, https://doi.org/10.34616/150469.

[5] Z. Jóźwiak, *Sztuczna inteligencja zorganizuje przetarg? To wcale nie takie pewne*, "Prawo.pl" 2023, https://www.prawo.pl/biznes/wykorzystanie-sztucznej-inteligencji-w-zamowieniach-publicznych,522495.html (access: 3.07.2024).

This is especially true in cases where the effects of its action may affect the functioning of the state and the quality of life of its citizens. Cyber security and privacy aspects are also worth noting. To avoid potential legal problems, institutions and individuals using AI tools should pay attention to maintaining confidentiality and acting in accordance with regulations.

It should also be emphasised that, despite significant technological advances, the implementation of AI solutions in the public sector faces challenges such as ethical issues, transparency in the operation of algorithms, accountability for decisions taken, or potential errors found in training data. What is equally important is the skills of the sector's workforce and, linked to the development of the technology, the need for continuous training. However, increasing the use of AI in the public sector seems inevitable. Nevertheless, this requires creation of an appropriate legal framework that defines the scope of the use of such tools and ensures security both to citizens and public sector employees.

In this context, data protection is a particularly relevant legal aspect because the use of AI in the public sector often involves processing of large amounts of data, including sensitive data. Regulations such as the General Data Protection Regulation (GDPR) in the European Union (EU) impose strict data processing requirements that public institutions have to comply with.

In the face of an increasingly automated and robotic society, and given the direction in which artificial intelligence is developing, it is important to consider its legal status. The law needs to be adapted to those changes that are taking place in society and in the sphere of new technologies. It is also advisable to seek an answer to the following question: are regulations adequately tailored to the upcoming technological revolution?[6] The difficulties for the legal system as a whole in relation to the development of artificial intelligence are linked to the wider phenomenon of technological progress, which is a continuous and unstoppable process. The impact of these technological advances on almost every

[6] A. Konieczna, *Problematyka sztucznej inteligencji w świetle prawa autorskiego*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, No. 4, p. 107.

area of law can in no way be ignored and there is a need of constant adaptation of the law to changing realities.[7]

The public sector constitutes an important element owing to which society's needs can effectively be met: be it at local, regional, national, or international levels. Public entities increasingly carry out the tasks assigned to them while using ICT systems, which not only makes them more efficient but also reduces their costs and allows them to reach a wider group of recipients in a relatively short period of time.[8] Due to the fact that the public sector is a factor not only stimulating the process of providing social services but also enforcing certain behaviours of the participants of this process, it becomes important to manage this sphere appropriately.[9] Meeting societal needs effectively means greater use of artificial intelligence while maintaining safety standards.

One of the main problems in regulating the various aspects of artificial intelligence is its very definition. This is because it is still a novel and rapidly developing phenomenon. In this respect, especially in the context of the possibility of claiming compensation for damages caused by artificial intelligence, particular emphasis should be placed on the issue of its autonomy, which should determine the proper scope of such liability. The definition of artificial intelligence itself, as well as its different types: high or low risk, should also avoid casuistry. In view of the fact that it is troublesome to explicitly predict the direction which artificial intelligence will be developing in and the fields of its actual application, any proposal to regulate it should be taken with great caution.[10] Due

[7] P.P. Juściński, *Prawo autorskie w obliczu rozwoju sztucznej inteligencji*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, No. 1, p. 19.

[8] I. Hoffman, M. Karpiuk, *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex Localis – Journal of Local Self-Government" 2022, No. 3, p. 628.

[9] M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, No. 4, p. 8, doi: 10.36128/PRIW.VI47.751.

[10] P. Staszczyk, *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, "Europejski Przegląd Sądowy" 2022, No. 6, p. 29.

to the fact that artificial intelligence is a dynamic concept, it is problematic to propose a single definition of the term.[11]

The purpose of the present article is to analyse the current applications of AI in the public sector, to identify the main challenges and to provide an outlook for the further development of this technology. The article also aims to highlight the importance of adequate regulatory preparation. Particular attention will be paid to the legal aspects that are crucial for the safe and effective use of AI in the public sector. The research hypothesis adopted, on the other hand, assumes that an implementation of AI algorithms in the public sector is inevitable, which requires development of an appropriate legal framework that sets out rules for ethical and secure data processing, accountability and transparency of decision-making processes, and security principles.

In order to validate it, the Authors decided to conduct a source literature analysis and case studies. In addition, a detailed analysis of challenges and risks was carried out, focusing on cyber security, data protection, and legal aspects of the use of AI.

2. Areas of the use of artificial intelligence in the public sector

Techniques such as predictive analytics, machine learning, text analytics, and natural language processing (NLP) are used in this area. This enables collection and effective management of large data sets from dispersed sources such as sensors, social media, discussion forums, reports, or public records. This makes it possible to find patterns, trends and correlations, which, in turn, may support decision-making processes. As such, a key area where AI is applicable is big data analytics to understand and predict social and economic phenomena.[12]

[11] A. Popowska, *Prawo do autorstwa wytworów stworzonych przez sztuczną inteligencję*, "Przegląd Prawa Handlowego" 2024, No. 1, p. 46.

[12] N. Sghir, A. Adadi, M. Lahmer, *Recent advances in Predictive Learning Analytics: A decade systematic review (2012–2022)*, "Education and Infor-

As an example of the use of big data analytics, public health monitoring can be used to predict, prevent, and prepare for potential epidemics.[13] In the context of crime analysis, on the other hand, AI tools make it possible to predict and prevent crime based on the results of historical analysis and current information, identifying patterns and anomalies.[14] AI can also detect fraud in financial and tax sectors by analysing financial transactions in real time, allowing irregularities to be detected. It should be noted, however, that big data analyses only allow for the signalling of certain patterns and anomalies, which may signal, for example, a crime having been committed or a possibility of this and cannot be treated as an unambiguous diagnosis of the situation.

Another area of AI use in the public sector is an automation of administrative processes, which allows algorithms to perform routine and repetitive tasks. These are most frequently activities such as processing of applications for social benefits, licences, permits, or certificates. As a result, the efficiency of public services is increased, operating costs are reduced and waiting times for decisions are significantly reduced. In addition, AI helps to maintain and update databases and registers. Meanwhile, the use of chatbots makes public services accessible at all times and from any location. AI tools also play a key role in emergency management.

AI is also used in urban planning and transport management. On the other hand, an analysis of demographic, social, and environmental data and trends allows for optimal planning of infrastructure investments. As a support tool, AI is also used

mation Technologies" 2023, No. 7, p. 8300–8301, https://doi.org/10.1007/s10639-022-11536-0.

[13] N.L. Bragazzi et al., *How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 pandemic*, "International Journal of Environmental Research and Public Health" 2020, No. 9, 3176, p. 2–3, https://doi.org/10.3390/ijerph17093176.

[14] N. Shah, N. Bhagat, M. Shah, *Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention*, "Visual Computing for Industry, Biomedicine, and Art" 2021, No. 4(1), 9, p. 1–2, https://doi.org/10.1186/s42492-021-00075-z.

in education and healthcare systems. Digital tools may support the personalisation of learning processes and adapt them to the individual capabilities of the learner. In the context of the school sector, the potential applications of artificial intelligence extend beyond mere administrative efficiency. Meanwhile, in the health sector, algorithms support diagnostics and create individualised treatment plans for patients.[15] This support is made more effective by using data from wearable devices or mobile apps. Artificial intelligence has the potential to significantly enhance human well-being by improving the accessibility and efficiency of public services. For example, AI-driven platforms can provide real-time translation services for immigrants accessing health care or legal aid. However, ethical challenges remain, particularly concerning algorithmic bias, data privacy, and the risk of dehumanising public interactions. Governments must prioritise the development of ethical guidelines and frameworks to ensure that AI systems promote social equity and enhance, rather than replace, human decision making. A practical step could include establishing citizen advisory boards to review and provide feedback on the ethical implications of AI implementations.

A common area for the use of AI in all areas of the public sector is big data analytics, which allows for quick correlation finding and scenario building. However, it is important to emphasise that the use of AI capabilities in the public sector is evolving and, as a result, it is currently difficult to predict the exact use of this technology in the public sector in the future. At the same time, cyberspace is a new environment for humans, one which they are not evolutionarily adapted to. In addition, the pace of progress in ICT means that the use of digital tools, including AI, presents a number of challenges and risks, of which only some are known.[16]

[15] M. Bartusek, A. Kulawik, *Analiza potrzeb zastosowania nowoczesnej technologii i sztucznej inteligencji w sektorze ochrony zdrowia*, “Fides, Ratio et Patria. Studia Toruńskie” 2021, No. 15, p. 125–126.

[16] C. Banasiński (ed.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023, p. 23–24.

3. Legal determinants for the use of artificial intelligence in the public sector

In the European Union, an innovation package on artificial intelligence (including the GenAI4EU initiative, which aims to support new ways of using artificial intelligence in the private and public sectors) has been launched, which should not only be secure but also trustworthy. It also takes into account the need for its application in the public sector.

Given the fact that artificial intelligence systems may pose risks of various threats in the public sector, it is necessary for the legislator (whether international, EU, or national) to take this into account.

Inadequate risk management in the public sphere can lead to a number of breaches caused by the use of artificial intelligence, including information leakage, access to confidential data, unauthorised invasion of privacy, or disruption of ICT systems used by public entities. Risk management in the public sphere must therefore take into account the risks posed by the use of artificial intelligence, which must also be reflected in legal regulations, especially since public administrations are obliged to act on the basis of and within the limits of the law.

The implementation of artificial intelligence in public administration has already revealed several cases of cyber-incidents. For example, in 2023, a major public health agency faced disruptions due to an AI-driven scheduling system that prioritised incorrect patient data, leading to delays in emergency services. Another example involves a biometric identification system used at a national border crossing, which malfunctioned due to data poisoning attacks, causing significant delays and privacy violations. These incidents highlight the need for robust cybersecurity measures and contingency planning in case of AI system failures.

In Article 13, the Artificial Intelligence Act[17] explicitly stipulates that high-risk artificial intelligence systems should be designed in such a way that their operation is sufficiently transparent to enable users (including those in the public sector) to interpret the results of the operation of the systems and to use them appropriately. This is also to achieve compliance with the relevant user and provider obligations. High-risk artificial intelligence systems must also be accompanied by a user manual in a suitable digital (or any other) format that contains concise, complete, correct, and clear information that is relevant, accessible, and understandable to users.

High-risk artificial intelligence systems, according to Annex III of the Artificial Intelligence Act, are artificial intelligence systems used, *inter alia*, in the following areas: 1) identification and biometric categorisation of individuals; 2) management and operation of critical infrastructure; 3) access to and use of public services and benefits; 4) law enforcement; 5) border control; 6) administration of justice. Activities in this area fall within the public sphere.

What is being advocated is to build and strengthen the core capabilities and knowledge of artificial intelligence in the European Union, including the creation and strengthening of high quality data assets and appropriate data sharing mechanisms, which also applies to public administrations, and this is expected to maximise benefits for European society and the economy. AI-based solutions and data may not breach the principle of privacy and security as early as in their design phase, and must comply with data protection and ethical rules.[18]

The Artificial Intelligence Act, in Article 5, paragraph 1, letter (c), makes it clear that artificial intelligence practices such as marketing, commissioning, or use of artificial intelligence

[17] Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206#footnote63 (access: 14.07.2024).

[18] Art. 5 of Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the “Digital Europe” Programme and repealing Decision (UE) 2015/2240 (Official Journal of the EU L 166, pp. 1–34).

systems by or on behalf of public authorities for the purpose of assessing or rating the reliability of individuals conducted over a period of time on the basis of their social behaviour or known or predicted personal or personality traits are prohibited where the said assessment leads to the following: 1) prejudicial or unfavourable treatment of some individuals or whole groups of individuals in given social circumstances that are unrelated to the circumstances in which the data was originally generated or collected; 2) prejudicial treatment of some individuals or whole groups of individuals that is unjustified or disproportionate to their social behaviour or its significance.

What is also prohibited, in the field of artificial intelligence, is the use of real-time remote biometric identification systems in public spaces for law enforcement purposes, except to the extent that such use is absolutely necessary for one of the following purposes: 1) search for victims of crime, including missing children; 2) prevention of a specific, serious, and imminent threat to the life or safety of an individual or a terrorist attack; 3) detection, location, identification, or prosecution of the perpetrators or suspects of certain offences that are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years under the law of the Member State concerned. This prohibition, and exceptions to it, derive from Article 5, paragraph 1, letter (d) of the AI Act.

The public authority, as a provider[19] of high-risk artificial intelligence systems, has, according to Article 16 of the Artificial Intelligence Act, an obligation to: 1) ensure that the system complies with legal requirements; 2) possess a quality management system; 3) draw up technical documentation; 4) keep records of events; 5) ensure that such a system undergoes an appropriate conformity assessment procedure before being placed on the market or put into service; 6) register that system in an EU database;

[19] A provider means, among other things, a public authority that develops an artificial intelligence system or has it developed with a view to marketing it or putting it into service under its own trade name or its own trademark – whether in return for payment or free of charge, Art. 3, item 2 of the Artificial Intelligence Act.

7) take necessary corrective action; 8) display a label indicating that the system complies with specific requirements.

The question of who is responsible for actions taken by artificial intelligence systems remains a contentious issue in legal discussions. While the system provider is required to ensure compliance with legal and technical standards, the ultimate responsibility may also lie with the public sector entity deploying the system. For example, if an AI algorithm used for public service allocation unintentionally discriminates against specific groups, liability could extend to both the algorithm's developers and the public officials overseeing its deployment. Clarifying these responsibilities requires both national legislation and international guidelines that address the shared and distinct roles of various actors in AI governance.

To a greater extent, however, actors from the public sphere will be users[20] of artificial intelligence systems rather than providers. As users of emotion recognition systems or biometric categorisation systems, they have an obligation to inform those individuals to whom these systems are applied of the fact that they are being used. However, it should be emphasised that this obligation is excluded in the case of artificial intelligence systems used for biometric categorisation for the purpose of detecting, preventing, and investigating crimes, where this is prescribed by law. Users of an artificial intelligence system that generates images, audio content, or video content that confusingly resembles existing persons, objects, places, or other entities or events, or one that manipulates such images and content so that the person receiving them might wrongly believe them to be authentic or real (i.e. "deepfake"), shall disclose that such content has been generated or manipulated by an artificial intelligence system. These obligations of public authorities derive from Article 52, paragraphs 2–3 of the Artificial Intelligence Act.

Innovative artificial intelligence systems, as stated in Article 54, paragraph 1, letter (a) of the Artificial Intelligence Act,

[20] A user includes a public authority that uses an artificial intelligence system under its control, Art. 3, item 4 of the Artificial Intelligence Act.

shall be developed to ensure the protection of an important public interest, such as: 1) prevention, preliminary proceedings, detection, or prosecution of crime or enforcement of criminal penalties. What is public interest here is protection against and prevention of threats to public safety under the supervision and responsibility of competent authorities; 2) public security and public health, which should include prevention, control, and treatment of diseases; 3) a high level of the protection and improvement of the quality of the environment. Personal data collected for other purposes may be processed for the development and testing of innovative artificial intelligence systems to protect an important public interest.

It should be emphasised that the very rapid development of artificial intelligence, robotics, and related technologies, including advances in software and the handling of large amounts of data produced or generated, as well as the development of technical machine learning, poses a major challenge to legislation in relation to the need for the law to keep up with the speed of changes in its social and technological environment.[21] This challenge is faced both by international, EU, and national legislators.

Issues related to public sector responsibilities for the safe use of artificial intelligence tools are governed by the Convention on Artificial Intelligence and relate to ensuring that activities within the life cycle of artificial intelligence systems are fully compatible with human rights, democracy, and the rule of law.[22]

Each Party shall apply this Convention to the life cycles of artificial intelligence systems undertaken by public authorities.

The policy on the development of artificial intelligence in Poland and protection against the risks of its misuse must take into account the public sector, which has a very strong impact

[21] R. Stefanicki, *Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana*, "Przegląd Prawa Handlowego" 2023, No. 1, p. 9.

[22] Art. 1, item 1 and Art. 3, item 1 of the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, https://secure.ipex.eu/IPEXL-WEB/download/file/082d29089070f71e01907839bb9d0be5 (access: 09.07.2024).

not only on the performance of public tasks but also on the economic sphere. Artificial intelligence, due to the need to streamline the operation of public administration and reduce the costs of its functioning, should also be used in processes (including decision-making) occurring in the public sphere. However, it is important to keep in mind the constant control of the operation of artificial intelligence tools, which must be used for their intended purpose.

Nowadays, ICT systems are not only used to retrieve information but also to carry out various types of activities; with the use of these, public tasks are performed. In some cases, they are of strategic importance for the state and the economy. They must therefore be duly protected, sometimes at the expense of human freedoms and rights.[23]

The public sector's use of artificial intelligence tools must be secure; it must be properly protected against cyber threats that can even paralyse the work of individual offices. Ensuring cyber security in the public sector that uses artificial intelligence systems must constitute a priority in a digitalised state.

Recital 51 of the Artificial Intelligence Act makes it clear that cyber security plays an important role in ensuring that artificial intelligence systems are resilient to attempts by malicious third parties acting in bad faith to modify their application, behaviour, performance, or circumvent their safeguards by exploiting vulnerabilities in the system. Cyber attacks on artificial intelligence systems may involve an exploitation of specific resources or vulnerabilities in the digital resources of an artificial intelligence system or in the ICT infrastructure which the system relies on. To ensure a level of cyber security appropriate to the risk, providers of high-risk artificial intelligence systems should implement appropriate measures, also taking into account the underlying ICT infrastructure.

Due to the potential cyber threats and their consequences, high-risk artificial intelligence systems will be of a particular impor-

[23] M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, No. 3, p. 40. doi: 10.17951/sil.2022.31.3.31-43.

tance, and this also applies to public administrations, including those performing security and public order tasks.[24] Accordingly, Article 15, paragraph 1 of the Artificial Intelligence Act requires that such systems are designed and developed to achieve, given their purpose, an appropriate level of accuracy, reliability, and cyber security and to perform consistently in these respects throughout their life cycle. Cyber security protects against cyber threats and thus ensures, on many levels, normal functioning of the state, as well as facilitates business operations.[25] It also protects against the negative impact of artificial intelligence on the cyberspace used to fulfil the mission entrusted to the public sector.

Artificial intelligence can be used in the field of critical infrastructure management, which relies heavily on ICT systems. Consequently, attention must be paid to ensuring the security of the operation of these systems. Their cyber security will therefore be important in this case.

It should be emphasised that ICT systems used in connection with the operation of critical infrastructures must be resilient to cyber threats, as services of strategic importance to the state and society are provided through them.[26]

4. Conclusions

Artificial intelligence in the public sector offers a wide range of opportunities to improve the quality and efficiency of services: from data management to the automation of administrative processes. AI supports big data analyses, making it possible to predict social and economic phenomena, as well as to monitor public health and crime. Automation of administrative tasks with AI improves opera-

[24] D. Skoczylas, *Krajowy System Cyberbezpieczeństwa*, Warszawa 2023, p. 9.

[25] M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, No. 2, p. 190, doi: 10.17951/sil.2023.32.2.189-201.

[26] M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, No. 5, p. 49, doi: 10.17951/sil.2023.32.5.43-52.

tional efficiency and reduces the delivery time of public services. In emergency management, AI enables rapid response to emergency situations and, in urban planning and transport management, it optimises traffic control systems and infrastructure planning.

However, the implementation of AI brings about significant challenges, including ensuring the security of AI systems, personal data protection and the need to comply with legislation such as GDPR. The security of AI technologies is crucial due to the vulnerability to cyber attacks, which may lead to major disruptions in the functioning of the state. Transparency in the operation of algorithms and accountability for decisions taken are also important ethical and regulatory considerations. In addition to the risk of opacity, there is also the risk of privacy. As previously stated, artificial intelligence systems can process a substantial quantity of data. However, the pairing of AI and data gives rise to a complex balancing act with regard to personal data, particularly in the context of automated processing.

Increasing the use of AI in the public sector requires adequate regulatory preparation and continuous improvement of staff skills. The research hypothesis that an implementation of AI algorithms in the public sector is inevitable is confirmed by the analysis conducted in the article. This is due to the growing need to increase the efficiency and quality of public services and the potential of AI in these areas. However, in order for the implementation of AI to be effective and secure, it is necessary to develop an appropriate legal framework that ensures ethical and secure data processing, accountability for decision-making processes, and transparency in the operation of algorithms. Appropriate regulations and ensuring a high level of security and ethics in the operation of AI are very important for its effective and safe implementation in the public sector.

Achievements in artificial intelligence are evident in every field.[27] Some results are also evident in the public sphere, yet modern solutions are unfortunately arriving there with a delay, which

[27] S. Wojtczak, P. Księżak, *Prawo autorskie wobec sztucznej inteligencji (próba alternatywnego spojrzenia)*, "Państwo i Prawo" 2021, No. 2, p. 18.

also hampers the development of this sphere and limits the possibilities of contact with the public in particular via ICT systems.

Artificial intelligence should be used to a greater extent in the fight against threats (without generating threats itself). Its algorithms can support the process of predicting threats and eliminating them even before undesired effects have been caused. It can also be applied to dealing with their consequences and prevention of these in the future.

Artificial intelligence cannot be considered in isolation from cyber security. The use of advanced digital technologies, while applying artificial intelligence tools, must be secure.

The role of cyber security and personal data protection in a digital society requires a holistic approach that takes into account, in addition to the ICT infrastructure and the level of digital competence of the population, a number of other factors, such as the security environment or the international situation, among others.[28]

A public administration that makes use of new technologies and effectively implements artificial intelligence tools will not only develop but will also respond to the expectations of the information society, which makes extensive use of cyberspace for its activities.[29] This process, however, not only has to comply with the law but also with ethical standards. In addition to the risk of opacity, there is also the risk of privacy. As previously stated, artificial intelligence systems can process a substantial quantity of data. However, the pairing of AI and data gives rise to a complex balancing act with regard to personal data, particularly in the context of automated processing.

To align national regulations with the EU Artificial Intelligence Act, it is necessary to introduce specific legislative measures. These should include mandatory training programmes for pub-

[28] K. Kaczmarek, M. Karpiuk, C. Melchior, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, No. 3, p. 119–120.

[29] M. Karpiuk, *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, No. 4, p 166–169.

lic officials on AI ethics, security protocols, and data protection. Additionally, a dedicated oversight body could be established to monitor AI applications in the public sector, ensuring compliance with transparency and accountability requirements. Such measures would not only enhance the legal framework but also build public trust in AI-driven public services.

In summary, AI has a great potential to improve the operational efficiency and the quality of public services. Realising this potential requires a well-balanced approach that takes into account both the benefits and the existing challenges and risks. Creating appropriate regulations and ensuring a high level of security and ethics in the operation of AI are key to its effective and safe implementation in the public sector.

Finally, it needs to be emphasised that the final decision-making process should constitute a human-led activity, one which may only be supported by artificial intelligence.[30]

SUMMARY

Use of artificial intelligence in public sector: threats and prospects

The aim of the article is to analyse the possibilities of using artificial intelligence in the public sector and to identify both the opportunities and threats posed by this digital tool. The authors showed that, thanks to advanced data analysis capabilities, automation of administrative processes, and crisis management, AI can significantly improve the efficiency and quality of public services. However, the implementation of this technology in the public sector is associated with several challenges, including system security, personal data protection, and transparency of decision-making processes. In the conclusions, the authors emphasise that the implementation of artificial intelligence in the public sector requires a balanced approach that takes into account both benefits and risks.

Keywords: public sector; artificial intelligence; security

[30] P. Fik, P. Staszczyk, *Sztuczna inteligencja w unijnej koncepcji e-sprawiedliwości – teoria i możliwy wpływ na praktykę*, "Europejski Przegląd Sądowy" 2022, No. 7, p. 9.

STRESZCZENIE

Wykorzystanie sztucznej inteligencji w sektorze publicznym. Zagrożenia i perspektywy

Celem artykułu jest analiza możliwości wykorzystania sztucznej inteligencji w sektorze publicznym oraz identyfikacja zarówno szans, jak i zagrożeń, jakie niesie ze sobą to cyfrowe narzędzie. Autorzy wykazali, że dzięki zaawansowanym możliwościom analizy danych, automatyzacji procesów administracyjnych i zarządzania kryzysowego AI może znacząco poprawić efektywność i jakość usług publicznych. Wdrożenie tej technologii w sektorze publicznym wiąże się jednak z szeregiem wyzwań dotyczących m.in. bezpieczeństwa systemów, ochrony danych osobowych oraz przejrzystości procesów decyzyjnych. We wnioskach autorzy podkreślają, że implementacja sztucznej inteligencji w sektorze publicznym wymaga zrównoważonego podejścia, które uwzględnia zarówno korzyści, jak i ryzyka.

Słowa kluczowe: sektor publiczny; sztuczna inteligencja; bezpieczeństwo

BIBLIOGRAPHY

Adadi A., Lahmer M., *Recent advances in Predictive Learning Analytics: A decade systematic review (2012–2022)*, “Education and information technologies” 2023, No. 7. https://doi.org/10.1007/s10639-022-11536-0.

Banasiński C. (ed.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023.

Bartusek M., Kulawik A., *Analiza potrzeb zastosowania nowoczesnej technologii i sztucznej inteligencji w sektorze ochrony zdrowia*, “Fides, Ratio et Patria. Studia Toruńskie” 2021, No. 15.

Blicharz J., Zacharko L., *Wdrażanie technologii sztucznej inteligencji w administracji publicznej – kilka refleksji*, in: P. Lisowski (ed.), *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, Wrocław 2024, https://doi.org/10.34616/150469.

Bragazzi N.L., Dai H., Damiani G., Behzadifar M., Martini M., Wu J., *How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 pandemic*, “International journal of environmental research and public health” 2020, No. 9, https://doi.org/10.3390/ijerph17093176.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, No. 5, doi: 10.17951/sil.2023.32.5.43-52.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, No. 3, doi: 10.17951/sil.2022.31.3.31-43.

Fik P., Staszczyk P., *Sztuczna inteligencja w unijnej koncepcji e-sprawiedliwości – teoria i możliwy wpływ na praktykę*, "Europejski Przegląd Sądowy" 2022, No. 7.

Hoffman I., Karpiuk M., *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex Localis – Journal of Local Self-Government" 2022, No. 3.

Jóźwiak Z., *Sztuczna inteligencja zorganizuje przetarg? To wcale nie takie pewne*, "Prawo.pl" 2023. https://www.prawo.pl/biznes/wykorzystanie-sztucznej-inteligencji-w-zamowieniach-publicznych,522495.html.

Juściński P.P., *Prawo autorskie w obliczu rozwoju sztucznej inteligencji*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, No. 1.

Kaczmarek K., Karpiuk M., Melchior C., *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, No. 3.

Kaplan A., Haenlein M., *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, "Business Horizons" 2019, No. 1, https://doi.org/10.1016/j.bushor.2018.08.004.

Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, No. 4, doi: 10.36128/PRIW.VI47.751.

Karpiuk M., *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, No. 4.

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, No. 2, doi: 10.17951/sil.2023.32.2.189-201.

Konieczna A., *Problematyka sztucznej inteligencji w świetle prawa autorskiego*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, No. 4.

Popowska A., *Prawo do autorstwa wytworów stworzonych przez sztuczną inteligencję*, "Przegląd Prawa Handlowego" 2024, No. 1.

Shah N., Bhagat N., Shah M., *Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention*, "Visual

Computing for Industry, Biomedicine, and Art" 2021, No. 4, https://doi.org/10.1186/s42492-021-00075-z.

Skoczylas D., *Krajowy System Cyberbezpieczeństwa*, Warszawa 2023.

Staszczyk P., *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, "Europejski Przegląd Sądowy" 2022, No. 6.

Stefanicki R., *Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana*, "Przegląd Prawa Handlowego" 2023, No. 1.

Wang Y., Sun T., Li S., Yuan X., Ni W., Hossain E., Poor H.V., *Adversarial Attacks and Defenses in Machine Learning-Powered Networks: A Contemporary Survey*, https://ar5iv.labs.arxiv.org/html/2303.06302.

Włodyka E.M., *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce*, in: M. Karpiuk (ed.), *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, Warszawa 2024.

Włodyka E.M., *Sztuczna inteligencja w sektorze publicznym – stan i oczekiwania*, in: L.J. Maksymowicz, Z. Danielewicz (eds.), *Edukacja, komunikacja i dyskursy społeczne. Studia humanistyczne i społeczne*, Koszalin 2023.

Wójcik M., *Sztuczna inteligencja: potencjał dla procesów zarządzania informacją*, "Przegląd Biblioteczny" 2017, No. 1.

Wojtczak S., Księżak P., *Prawo autorskie wobec sztucznej inteligencji (próba alternatywnego spojrzenia)*, "Państwo i Prawo" 2021, No. 2.