Teka Komisji Prawniczej PAN Oddział w Lublinie
vol. XIX, 2026, no. 1, pp. 7-21
https://doi.org/10.32084/tkp.10665

SECURITY OF PUBLIC ADMINISTRATION IN THE AGE OF AI. COMPARATIVE ANALYSIS

Dr. Dawid Chaba

University of the National Education Commission in Kraków, Poland
e-mail: dawid.chaba@uken.krakow.pl; https://orcid.org/0000-0002-2385-3466

Dr. habil. Kazimierz Bandarzewski, University Professor

Jagiellonian University in Kraków, Poland
e-mail: kazimierz.bandarzewski@uj.edu.pl; https://orcid.org/0000-0002-8783-8820

Abstract. The authors comparatively analyze the impact of artificial intelligence (AI) on security in public administration. The rapid advancement in AI technology offers new opportunities, but it also entails significant risks for the public sector. The analysis covers the current use of artificial intelligence in administration, the risks associated with the introduction of artificial intelligence into public administration, plans for the future and challenges in Poland, the United States and China. To ensure the safe use of AI, it is necessary to conduct a broad discussion on the scope of implementation of AI in the functioning of public administration and, on this basis, to define a regulatory framework. The topic requires an interdisciplinary approach, combining computer, legal and public policy knowledge. The article addresses the critical issue of the impact of AI systems on the security of public administration, a key problem for the responsible and effective implementation of technological innovations in the public sector. The proposed interdisciplinary approach combines artificial intelligence, legal and ethical knowledge and public policy. It can contribute to the development of comprehensive solutions for the safe use of AI in public administration, in line with the public interest.

Keywords: artificial intelligence; public sector governance; cybersecurity; AI regulations.

INTRODUCTION

The computerization of public administration significantly changes the ways of management and approach to security. Artificial intelligence (AI) is a field of information technology that is of increasing interest to researchers, businesses and administrations. Its dynamic development opens the way to new, practical opportunities in virtually every area of social and economic life. The concept of AI is defined in European Union law as a machine system that has been designed to operate with varying levels of autonomy once

ISSN 1899-7694
e-ISSN 2719-7379

it has been implemented and that can be adaptable once it has been implemented, and which, for explicit or implied purposes, infers how to generate results such as predictions, content, recommendations or decisions from the input data obtained. That may affect the physical or virtual environment (Article 3(1) of Regulation No. 2024/1689). Although this act will not enter into force until 2 Augus. 2026, Member States are already making attempts to enact national legal acts regulating the use of AI and adapting this regulation to their own legal systems (Draft Act on Artificial Intelligence Systems. 2024). Importantly, the above-mentioned Regulation No. 2024/1689 clearly distinguishes AI from simpler, traditional software systems or programming assumptions, indicating that this concept should not include systems based on rules defined only by natural persons for the purpose of automatic operation (thesis No. 12 of Regulation No. 2024/1689). One of the essential characteristics of AI is its ability to make inferences involving both the process of obtaining outcomes such as predictions, content, recommendations or decisions that can affect the physical and virtual environment and the ability of AI to create models or algorithms based on input information or data. AI, through its ability to make independent conclusions, becomes an intelligence independent of humans and capable of acting without humans, including self-learning [Kamiński 2023].

Public administration is one of those sectors where artificial technology will be used in the future. In the age of artificial intelligence, public administration can increasingly use new technologies for decision-making, communication with the public and resource management. IT systems that improve or automate public services, data analysis, infrastructure management and fraud prevention significantly improve the functioning of the state. They should improve the quality of public services and help reduce common bureaucratic problems [Blicharz and Zacharko 2024].

However, the introduction of AI into administrative structures brings new risks, particularly in terms of the protection of fundamental rights, cybersecurity, data protection and the violation of the principles of equality and justice, and thus legality, which in turn is essential for the proper functioning of the administration. Improperly designed or unsupervised AI systems have the potential to cause infringements of personal rights, discrimination against social groups, perpetuation of inequalities and violation of the rights of persons (parties) using administrative services.

History knows precedents where algorithms used in the judiciary, HR, or credit background checks have relied on human biases encoded in training data [Wirtz, Weyerer, and Geyer 2018].

The article aims to diagnose the impact of artificial intelligence on the security of public administration, comparing the situation in Poland, the United States and China. At the same time, the assessment of this impact on the

activities of the administration in Poland will be of particular importance. This sample selection is due to the varying level of public sector AI deployment in these countries, their different legal and cultural environments, and their important international position in terms of technology trends.

1. SIGNIFICANT RISKS ASSOCIATED WITH THE USE OF AI IN ADMINISTRATIVE ACTIVITIES

The challenges and risks associated with AI systems, especially those related to security, need to be properly managed so that the benefits of AI in public administration can thrive. Privacy and confidentiality of personal data processed by artificial intelligence is essential. The public sector deals with particularly sensitive information, such as medical, financial, forensic or housing records. Any leakage or misuse of data as a result of a hacking attack, insufficient security, or human error has consequences for individuals and the integrity of the state [Madan 2022]. The challenge is to ensure the transparency and accountability of AI systems supporting decision-making processes in the public sector. Many deep neural networks act as "black boxes": they process inputs and produce specific results, but how they do this remains a mystery to their creators. Algorithms influencing administrative decisions in areas such as social welfare, licences, permits or fines must guarantee citizens the right to clear justification for their decisions. The lack of transparency in the operation of AI systems in public administration undermines trust in public institutions and creates a risk of impunity for officials hiding behind algorithmic recommendations [Snopkiewicz 2020].

Public administration is a set of organizational and executive activities aimed at the implementation of the common good, related to the basis and forms of action by law [Niewiadomski 2010]. The activity of public administration is largely individual. The authority decides on the case of a specific person, and this decision is made by issuing an individual administrative act. This form of administrative activity is and will be one of the basic planes of its functioning in the future, because it establishes the basic element of the administrative relationship, which is the inequality of the parties [Filipek 1995]. The issuance of an individual administrative act allows not only to clearly specify the rights and obligations of a given person, but also to clarify the actions of the authority and ensure the greatest possible protection of such a person through the possibility of lodging appeals.

Quite often, in studies on the use of AI in administration, this aspect of its activity is omitted, and it is crucial in its functioning. Thus, ensuring security at the stage of conducting individual administrative cases should be treated as the basic scope of this security [Ziółkowska and Wierzbowski 2022].

Artificial intelligence as a machine learning system must be based on a large (very large) amount of data. It is reasonable to say that machine learning algorithms are just as good as the training data they are fed with. Thus, the risk of transferring human biases, stereotypes and cognitive biases from training data to artificial intelligence systems used in public administration is serious [Konopka 2023].

At the same time, an extremely important risk related to the very functioning of the administration is overlooked, consisting in the fact that there are sometimes millions of individual administrative decisions in legal transactions, issued in individual cases, sometimes repeated, and sometimes completely different. For example, in 2023, the local government administration of the City of Krakow alone issued over 816 thousand administrative decisions (Krakow in numbers. 2023). This is another significant threat associated with the use of AI by public administration. However, it is not about the number of such decisions, but about the possibility of AI 'learning' on such data sets. It may turn out that in the same circumstances, several hundred rulings favourable to the parties were issued, but also a similar number of negative rulings to the parties [Kozłowski 2023]. What kind of model is artificial intelligence supposed to develop then? Based on historical data, AI can develop its 'own' discrimination system at the algorithm level [Skuza and Lizak 2023]. Furthermore, it must be noted that the discriminatory patterns themselves are not permanent. Whether a given characteristic is discriminatory or not discriminatory is decided by the legislator, who sometimes directly grants more or less rights to persons with certain characteristics.

Another threat to the use of AI systems in public administration is the specificity of its activity consisting in justifying the issued decisions. A decision or other administrative act does not consist only of the decision itself, but sometimes a very extensive justification sometimes even several dozen pages long. The justification of administrative decisions should consist of the justification of the factual and legal parts. In practice, the justifications for administrative decisions may not contain these parts, or they may be mixed together or even incomprehensible.

Another threat not indicated in the doctrine is the occurrence of many unlawful decisions in legal transactions [Bamberger 2010]. Each party demanding a specific decision will fully accept it also if it is favorable to it but against the law. No appeals will be lodged against such a decision and it will function in legal transactions.

In addition to obvious (gross) illegality, in the legal transactions of each country there is a very large number of decisions that violate the law to an insignificant degree. Such decisions, even if subject to judicial review, will not be eliminated from legal circulation due to the fact that the degree of violation of the law is not high.

Another issue pointing to the threats to the introduction of AI in administration is its decentralization and the use of both discretionary decisions, as well as general clauses and vague concepts. Increasingly, public administration is decentralised in order to best meet the needs of specific residents. These needs may be similar, but the way of satisfying them is diverse and the greater the scope of independence of local administration, the different the decisions may be. The admissibility of using AI in cases that end with the issuance of so-called discretionary decisions is already indicated as extremely controversial [Sibiga 2019]. In the case of discretionary decisions, the outcome of the case is not directly related to the established facts and legal status. Thus, it may turn out that in two practically identical states of affairs, the authorities make different decisions. If the justification for such decisions sufficiently states the reasons for such different actions, then this poses a threat as to how AI will 'learn' how to resolve such cases. It may turn out that the difference in these decisions is based on the application of the so-called general clauses such as 'public interest' or 'legitimate interest of a party' and without explaining what it consists in a given case. Then AI itself will have to define such a concept for the needs of a specific case. This will be extremely difficult, because defining a general clause (e.g. public interest) cannot be based on generalizing this concept from already issued decisions. This will require skipping a number of use cases, which seems to be difficult to program for an AI system.

Accountability for autonomous AI decisions and potential harms is a fundamental legal and ethical challenge for their implementation. Under current laws, officials and authorities are responsible for their decisions [Butt 2024]. However, the involvement of machine learning algorithms in these decisions complicates matters because they are not always completely predictable and transparent.

2. AI IN PUBLIC ADMINISTRATION

The security of data and systems, the scope of data entered into the AI system and constant control over the activities of AL are of key importance for the functioning of AI systems in public administration. Polish public administration is facing many challenges related to digitization and implementation of AI. The lack of integrated security strategies and a non-standard approach to risk management threaten the integrity of the administrative system. Polish legislation emphasizes the protection of personal data, primarily due to the implementation of the General Data Protection Regulation (GDPR), but data protection should be adapted to AI, because the artificial intelligence system can also 'deanonymize' (decode) personal data while learning on its own. Artificial intelligence is beyond the capabilities

of the human mind, so it can identify people who seem to be safe after the anonymization process based on a lot of data [Jakubik and Prabucki 2024]. A significant problem remains the lack of professional staff and infrastructure, which makes the Polish administration vulnerable to cyberattacks.

Artificial intelligence has become increasingly important in public administration in the United States, and the government has passed many laws to ensure data security. Legislation such as the Cloud Act and the Cybersecurity and Infrastructure Security Agency Act focuses on improving the security of digital infrastructure and protecting against cyber threats [Chaba 2024]. U.S. public authorities, such as the Department of Homeland Security, actively work with the private sector to ensure the security of administrative systems.

Despite these improvements, some researchers have expressed concerns about the impact of artificial intelligence to privacy, especially in the context of data collection in surveillance systems [Androniceanu 2023]. China's approach to security in public administration in the field of AI is completely opposite. It makes widespread use of artificial intelligence in city management and planning and in mass surveillance, including the 'social credit' system [Madan 2022]. While these systems are effective in supporting the administrative activities and management of agglomerations, they raise concerns about excessive surveillance and a lack of individual privacy protection. The Chinese government has made extensive use of measures to protect digital infrastructure, but it has often been criticized for restricting rights [Chen, Ran, and Gao 2019]. Further sections examine the use of AI in the public administrations of the countries concerned.

2.1. Poland

Poland is at a very early stage of implementing AI solutions in its public administration. Her experience to date is mainly trial and experimental programs at selected institutions [Dudzik, Kawka, and Śliwa 2024]. One of them is a chatbot that answers common questions and informs citizens about official procedures. The Ministry of Finance has such a chatbot [Kuziemski and Misuraca 2020]. Another testing ground for artificial intelligence algorithms is data analysis for tax services. Machine learning tools are designed to support the selection of entities for inspection, detect errors in tax returns and identify financial fraud, e.g. VAT [Dudzik, Kawka, and Śliwa 2024].

One of the steps towards the wider use of AI in the Polish public sector is the government's platform for data processing and the development of AI-based tools. The aim of the project is to build a central IT infrastructure and data resources for public institutions. The platform would integrate distributed state databases, offer data analysis tools, and help build and deploy

applications with integrated AI algorithms. This would enable offices to take advantage of economies of scale without the burden of high infrastructure costs and the requirement of appropriate competences [Kowalczyk 2021].

The government plans to use AI systems in the Polish administration mainly to improve communication with citizens and automate repetitive processes [Kuziemski and Misuraca 2020]. AI algorithms will help in making administrative decisions regarding social benefits, licenses, permits or fines [Kowalczyk 2021].

The implementation of ambitious plans for the digital transformation of the Polish public sector powered by artificial intelligence will not be possible if numerous challenges and barriers are not addressed. One of them is the low digital competence of officials who would launch and supervise artificial intelligence systems. Implementing advanced technology requires the right hardware and software infrastructure, but more importantly, it requires personnel with the right knowledge and skills. On the other hand, a significant proportion of public administration employees have no experience with AI, do not understand how it works and are not prepared to manage the risks it entails [Dudzik, Kawka, and Śliwa 2024]. Therefore, officials need intensive training and skills development to effectively use intelligent systems.

Another significant barrier is the lack of legal regulations on the use of artificial intelligence in the activities of public administration. The current legislation in Poland is far from taking into account the intricate nature of artificial intelligence systems and does not answer many questions about their implementation in the public sector. This is not an isolated situation. Generally, in European countries, procedures allowing the use of AI in the adjudication process are regulated only exceptionally, and only when the administrative act is a so-called related act and the authority does not have the discretion to assess the facts [Kamiński 2023].

The Polish legal system exceptionally allows for the automation of the administrative process, indicating the possibility of online transfer of information between a party or authority or in this mode of collecting evidence. Article 14(1b) of the Polish Code of Administrative Procedure, which has been in force since 2021, allows for the handling of cases using automatically generated letters and bearing a qualified electronic seal of a public administration body. Automatically generated letters are documents in electronic form that are created without direct or minimal human participation in the production of their document content and are the result of downloading and appropriate compilation of data by the ICT system, in particular based on data contained in public registers or provided by the applicant [Wilbrandt-Gotowicz 2021]. However, also in this regard, it is argued that handling cases using automatically generated letters without human intervention

(and thus in fact using artificial intelligence systems) does not apply to the issuance of administrative decisions [Knysiak-Sudyka 2023].

This does not mean that processes of highly advanced automation in administrative proceedings do not take place at all in Polish law. Since 2012, the Polish Social Insurance Institution has been deciding on the annual valorisation of pension benefits in a fully automated (and without human intervention) way, and since 2020 in the case of granting the so-called downtime benefits [Szyjewska-Bagińska 2022]. However, these examples of administrative proceedings cannot be considered the use of artificial intelligence, because there is no form of independent 'thinking' of the IT system, but only the automatic creation of a specific decision if precisely defined conditions are met.

It is also unclear how the transparency and accountability of administrative decision algorithms would be ensured, or how to assign responsibility for possible errors and damage caused by such autonomous systems [Kowalczyk 2021].

Therefore, comprehensive regulations are needed that will build a legal framework that promotes innovation and experimentation with new technologies in the public sector, while guaranteeing the highest standards of data, cybersecurity and protection of civil rights. One of the first regulations in the legal system will be the Act on Artificial Intelligence Systems (Draft Act on Artificial Intelligence, 2024), which is intended to apply Regulation No. 2024/1689. However, the primacy of man over the computer system should always be preserved, and not the other way around.

2.2. United States

The United States is a world leader in solutions based on artificial intelligence, also in the public sector. Machine learning algorithms are used in many areas of federal and state government, both in decision-making and in improving public services. U.S. Border and Immigration Services have particularly sophisticated artificial intelligence systems at their disposal to improve transnational traffic control, detect potential terrorist threats, and illegal immigration. One example is the controversial ATLAS system used by Immigration and Customs (ICE) authorities to automatically analyze data from social media and other sources to screen non-citizens for removal procedures [Engstrom, Ho, Sharkey, et al. 2020]. The American justice system is also increasingly using AI solutions. Parole courts and boards commonly use recidivism risk assessment tools when deciding on parole, bail amounts, or sentences [Di Vaio, Hassan, and Alavoine 2022]. Systems such as COMPAS, PSA, and LSI-R analyze a wide range of defendant data, such as their demographic profile and social or criminal history, to predict the likelihood of reoffending. Although the creators of the tools wanted to improve objectivity and reduce the impact of human bias on the justice system, there are

justified doubts about the actual reliability and impartiality of these systems towards representatives of various social groups [Skuza and Lizak 2023].

U.S. intelligence and homeland security institutions also use advanced artificial intelligence systems. Biometric data analysis algorithms for facial or hand geometry recognition are used in access control systems in sensitive government locations or to identify potential terrorists at airports. Another area of AI use is the analysis of large data inputs from electronic surveillance systems such as PRISM, which facilitates the identification of suspicious groups and aids in counterintelligence operations [Di Vaio, Hassan, and Alavoine 2022].

Moreover, AI systems are playing an increasingly important role in managing critical infrastructure in the United States, from power grids to transportation and water systems. IoT sensors and real-time data analysis algorithms can monitor infrastructure health, predict failures, and optimize maintenance and modernization of strategic assets [Engstrom, Ho, Sharkey, et al. 2020].

The future use of artificial intelligence in U.S. public administration is shaped by successive versions of national AI strategies. The current one is the National AI Initiative Act (NIAIA) of 2020,[1] which provides for increased federal spending on artificial intelligence research and implementation, cooperation between government agencies, and adaptation of innovative solutions in the public sector.

The U.S. administration focuses on building digital competencies for public sector employees. The United States Digital Service,[2] is expected to recruit highly skilled technology experts for government agencies to improve the digitization of public services. Dedicated training paths and university programs are designed to educate officials ready to implement and oversee machine learning-based systems [Engstrom, Ho, Sharkey, et al. 2020]. This confirms the thesis that staff competences are crucial for the correct and effective use of the potential of AI in administration.

The United States is also an active international agent in setting standards for the safe development of artificial intelligence. Its representatives are members of the OECD Working Group on Artificial Intelligence Governance, which has published recommendations and guidelines for governments on the responsible implementation of AI systems in line with human rights, democratic values and the principles of transparency [Grochmalski, Lewandowski, and Paszak 2020]. Internally, too, the United States is trying to establish a consistent legal framework and standards for the use of AI in the public sector. However, the federal structure and divergent regulations at the state level make this process difficult [Bullock, Young, and Wang 2020].

---

[1] U.S. Congress. House of Representatives. H.R. 6216 (116th Congress), https://www.congress.gov/bill/116th-congress/house-bill/6216 [accessed: 08.03.2026].

[2] U.S., U.S. Digital Service, https://www.usds.gov/ [accessed: 08.03.2026].

There is no shortage of challenges and controversies around the progressive 'algorithmization' of the American administration, especially given its current state. In addition to the threat to citizens' privacy discussed above from the development of AI-based surveillance and profiling systems, some critics question the transparency and neutrality of the tools used in justice or social welfare systems [Di Vaio, Hassan, and Alavoine 2022]. Civil rights concerned organizations warn that historical data used to train risk assessment algorithms could contaminate them with discriminatory patterns exposed in the justice system, such as disproportionately worse sentences for racial minorities [Bullock, Young, and Wang 2020]. The practical use of AI by the administration, e.g. in migration procedures, has been criticized due to the perpetuation of harmful stereotypes, as well as the bias of final decisions, which resulted from biased criteria as a consequence of the current political agenda [Molnar 2020].

It should be remembered that the development of AI in the US administration is influenced by strategic competition with China, which also aspires to become a world leader in this field. The pressures of technological competition can force decision-makers to prefer rapid deployment at the expense of security or system transparency.

2.3. China

China is today the undisputed world leader in artificial intelligence-based solutions. Beijing considers the development of artificial intelligence to be a strategic priority that is crucial to strengthening its international position and transforming its economic model towards innovative technologies. Fueled by colossal state and private investments worth billions of dollars and an unparalleled amount of data generated by a population of 1.4 billion, China has created an ecosystem of rapid development of machine learning. Flagship implementations of artificial intelligence in Chinese administration include smart city management, mass visual surveillance, advanced analytics for state security, and extensive e-government platforms [Wang, Teo, and Janssen 2021].

The idea of a smart city with a dense network of Internet of Things sensors, surveillance cameras, and real-time data analysis algorithms is widely used by those responsible for China's metropolises. AI systems for traffic optimization, energy efficiency of buildings, waste management or crisis response are exploited on a daily basis in cities such as Beijing, Shanghai and Shenzhen. Advanced facial recognition and behavioral analysis techniques can track people's movement, detect anomalies, and respond to potential threats [Roberts, Cowls, Morley, et al. 2021]. Still, the same infrastructure is part of an unprecedented surveillance and control mechanism.

A basic example is the social credit system in China, which has been operating since 2014. It is based on artificial intelligence algorithms that aggregate and analyze a wide range of citizen data, from purchase history and social media activity to traffic fines and loan repayment behavior. All this to calculate the 'credit' of a person. This assessment is intended to provide a synthetic measure of citizens' credibility and loyalty and affects their access to public services, career opportunities and travel. The system is integrated with pervasive surveillance and should promote 'virtues' and discourage 'bad deeds'. In essence, it is a tool of mass social engineering in line with the expectations of the Chinese Communist Party [Wu, Lu, Zhu, et al. 2020].

In 2017, the Chinese government adopted the ambitious Next Generation Artificial Intelligence[3] Development Plan, which aims to turn China into the undisputed world leader in the development and use of artificial intelligence by 2030. The plan envisages further intensifying research and development efforts to develop new applications for Artificial Intelligence in the public sector hand in hand with leading private technology companies such as Alibaba, Huawei, and Tencent. Its goal is to create an ecosystem of "smart state governance" in which AI algorithms are involved in every aspect of the relationship between the citizen and the state, from smart customer service in offices, to proactive information campaigns and tailor-made public services, to automated administrative decision-making [Wu, Lu, Zhu, et al. 2020].

One of the pillars of China's AI strategy is the development of facial recognition and behavior analysis technology, which is freely used by the state security system, especially in regions inhabited by minorities, such as Xinjiang and Tibet. Advanced AI is also being used to control the internet by identifying and blocking content deemed 'dissident' by the Great Firewall of China [Wang, Teo, and Janssen 2021].

The Chinese government is actively seeking exports of Chinese AI technology, including its controversial products, mainly through the Belt and Road Initiative. Smart city management systems, e-government platforms, and surveillance algorithms made in China are being deployed in Southeast Asia, Africa, and South America. Accepting countries do not always have regulations and safeguards in place to guarantee responsible use of tools [Wu, Lu, Zhu, et al. 2020]. The expansion of China's AI raises concerns about the "export of digital authoritarianism" and the technological dependence of developing countries on China [Grochmalski, Lewandowski, and Paszak 2020].

---

[3] State Council of the People's Republic of China. (2017). Full Translation: China's New Generation Artificial Intelligence Development Plan, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ [accessed: 08.03.2026].

While the widespread use of AI in China's public administration offers tangible benefits, such as optimized governance, it raises fundamental ethical and political concerns. Intelligent algorithms have become a tool of mass surveillance, invasion of privacy and unprecedented restrictions on civil liberties. China's history of using AI in the public sector demonstrates the potential of this technology as a tool for effective process management and optimization, but also as a serious threat if used for authoritarian control of the population and the suppression of civil liberties.

China's successful application of innovative AI solutions in state administration encourages other countries, including Poland, to consider the role of this technology in the modernization of public administration and services. Chinese inspiration in city optimization, healthcare, or predictive analytics can be valuable if the basic principles of democracy are followed and safeguards are applied. Copying China's model of AI "public surveillance" would be a violation of the values such as freedoms and individual rights on which liberal democracies are based. The example of China shows the need for civilian control and supervision over AI systems in administration. The system also requires the protection of privacy and anonymity in the era of big data, as well as the education of officials and citizens on the social consequences of technological solutions.

CONCLUSIONS

The article comparatively addresses the problem of the impact of AI systems on the security of public administration. The United States and China were selected together with Poland for their leading role in the global race for leadership in artificial intelligence. The United States is the birthplace of breakthrough innovations in artificial intelligence and neural networks. This is where tech giants such as Google, Microsoft, Amazon, and IBM have invested billions of dollars in the research and implementation of artificial intelligence. U.S. government agencies, such as the Defense Advanced Research Projects Agency, have been conducting advanced AI research for defense and security for decades. U.S. government is also eager to adopt machine learning-based solutions to predict crime, automate customer service, and detect tax fraud. China, on the other hand, is on track to become the world's leader in AI by 2030. They have a gigantic database of their citizens and are not as limited in their capabilities by regulatory safeguards as the West, which makes it easier to develop and implement machine learning systems. Chinese corporations such as Alibaba, Baidu, Tencent and SenseTime are investing heavily in AI research and are working closely with the government on a military-civilian fusion program.

AI plays a key role in China's research and public control mechanisms, as evidenced by mass surveillance and citizen scoring systems. AI is also widely used in China's public administration, from smart city management to the automation of e-government services. Compared to them, Poland is at an early stage of implementing and using AI in the public sector. So far, the projects that the country has undertaken have been attempts to focus on selected areas, such as chatbots for solving civic problems or analytical tools for tax services. There is a lack of a comprehensive strategy for the implementation of AI systems in public administration and an appropriate legal and ethical framework. Although the digital transformation of the Polish public sector is ongoing, it is lagging behind the technological leaders.

REFERENCES

Androniceanu, Armenia. 2023. "The new trends of digital transformation and artificial intelligence in public administration." *Revista Administratie si Management Public (RAMP)* 40:147-55.

Bamberger, Kenneth. A. 2010. "Technologies of Compliance: Risk and Regulation in a Digital Age." *Texas Law Review* 88:669.

Blicharz, Jolanta, and Lidia Zacharko. 2024. "Wdrażanie technologii sztucznej inteligencji w administracji publicznej – kilka refleksji." In *Administracja publiczna wobec procesów zmian w XXI wieku. Księga jubileuszowa Profesora Jerzego Korczaka*, edited by Piotr Lisowski, 349-56. Wrocław: Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Bullock, Justin, Matthew Young, and Yi-Fan Wang. 2020. "Artificial intelligence, bureaucratic form, and discretion in public service." *Information Polity* 25(4):491-506.

Butt, Junaid. 2024. "A Comparative Study About The Use Of Artificial Intelligence (AI) In Public Administration of Nordic states with other European Economic Sectors." *EuroEconomica* 43(1):40-66.

Chaba, Dawid. 2024. "Selected aspects of the use of artificial intelligence in public administration." *Roczniki Administracji i Prawa* XXIV(1):235-44.

Chen, Tao, Longya Ran, and Xian Gao. 2019. *AI innovation for advancing public service: The case of China's first Administrative Approval Bureau*. Proceedings of the 20th Annual International Conference on Digital Government Research.

Di Vaio, Assunta, Rohail Hassan, and Claude Alavoine. 2022. "Data intelligence and analytics: A bibliometric analysis of human–Artificial intelligence in public sector decision-making effectiveness." *Technological Forecasting and Social Change* 174:121201.

Dudzik, Sławomir, Inga Kawka, and Renata Śliwa. 2024. *E-administracja: Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej*. Kraków: Wydawnictwo Księgarnia Akademicka.

Engstrom, David. F., Daniel E. Ho, Catherine M. Sharkey, et al. 2020. *Government by algorithm: Artificial intelligence in federal administrative agencies*. NYU School of Law, Public Law Research Paper.

Filipek, Józef. 1995. *Prawo administracyjne. Instytucje ogóle*. Kraków: Universitas.

Grochmalski, Piotr, Piotr Lewandowski, and Paweł Paszak. 2020. "US-China technological rivalry and its implications for the Three Seas Initiative (3SI)." *European Research Studies Journal* XXIII(Special Issue 2):840-53.

Jakubik, Mateusz, and Rafał Prabucki. 2024. "Wykorzystywanie AI w administracji." https://szkolenia.administracjapubliczna.pl/blog/wykorzystywanie-ai-w-administracji/ [accessed: 08.03.2026].

Kamiński, Marcin. 2023. "Akt administracyjny zautomatyzowany. Zasadnicze problemy konstrukcyjne zastosowania systemów sztucznej inteligencji w procesach decyzyjnych postępowania administracyjnego na tle prawnoporównawczym." *Prawo i Więź* 4(47):282-300.

Knysiak-Sudyka, Hanna. 2023. *Kodeks postępowania administracyjnego. Komentarz*, edited by Hanna Knysiak-Sudyka, 3rd ed. Lex el.

Konopka, Maria. 2023. "'Każdy zna się na AI'. Przegląd badań polskiej opinii publicznej na temat sztucznej inteligencji." *Zeszyty Prasoznacze* 66, no. 4(256):127-42.

Kowalczyk, Marcin. 2021. *Cyfrowe Państwo. Uwarunkowania i perspektywy*. Warszawa: PWN.

Kozłowski, Jakub. 2023. "Ochrona praw podstawowych w przypadku stosowania sztucznej inteligencji przez administrację publiczną w Unii Europejskiej." In *Obywatel Citizen-centric w centrum działań e-Government e-administracji in the w Unii Europejskiej European Union*, edited by Sławomir Dudzik, Inga Kawka, and Renata Śliwa, 52-65. Kraków: Wydawnictwo Księgarnia Akademicka.

Kuziemski, Maciej, and Gianluca Misuraca. 2020. "AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings." *Telecommunications policy* 44(6):101976.

Madan, Rohit. 2022. *Artificial Intelligence Diffusion in Public Administration*. Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society.

Molnar, Petra. 2020. "AI and Migration Management." In *The Oxford Handbook of Ethics of AI*, edited by Marcus D. Dubber, Frank Pasquale, and Sunit Das. 777. New York: Oxford University Press.

Niewiadomski, Zygmunt. 2010. "Pojęcie administracji publicznej." In *System Prawa Administracyjnego*. Vol. 1: *Instytucje Prawa Administracyjnego*, edited by Roman Hauser, Zygmunt Niewiadomski, and Andrzej Wróbel, 1-60. Warszawa: C.H. Beck.

Roberts, Huw, Josh Cowls, Jessica Morley, et al. 2021. *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*. Springer International Publishing.

Sibiga, Grzegorz. 2019. *Stosowanie technik informatycznych w postępowaniu administracyjnym ogólnym*. Warszawa: C.H. Beck.

Skuza, Sebastian, and Robert Lizak. 2023. "Sztuczna inteligencja umożliwia kontrolę finansów publicznych – przegląd inicjatyw amerykańskiego rządu federalnego." *Białostockie Studia Prawnicze* 28(2):175-95.

Snopkiewicz, Konrad. 2020. "Przegląd zagrożeń w cyberprzestrzeni." *Studia Administracji i Bezpieczeństwa* 1(9):29-41.

Szyjewska-Bagińska, Joanna. 2022. "Prawne aspekty automatyzacji przyznawania i wypłaty świadczeń przez Zakład Ubezpieczeń Społecznych." *Praca i Zabezpieczenie Społeczne* 2:36-44.

Wang, Chanlin, Thompson S.H. Teo, and Marijn Janssen. 2021. "Public and private value creation using artificial intelligence: An empirical study of AI voice robot users in Chinese public sector." *International Journal of Information Management* 61:102401.

Wilbrandt-Gotowicz, Martyna (ed.). 2021. *Doręczenia elektroniczne. Komentarz*. Warszawa: Wolters Kluwer.

Wirtz, Bernd W., Jan C. Weyerer, and Carolin Geyer. 2018. "Artificial Intelligence and the Public Sector-Applications and Challenges." *International Journal of Public Administration* 42(7):596-615.

Wu, Fei, Cewu Lu, Mingjie Zhu, et al. 2020. "Towards a new generation of artificial intelligence in China." *Nature Machine Intelligence* 2(6):312-16.

Ziółkowska, Katarzyna, and Marek Wierzbowski. 2022. "Ocena wpływu wykorzystania sztucznej inteligencji w administracji publicznej." *Acta Universitatis Wratislaviensis* No 4101. "Prawo CCCXXXIV:505-13.