DOMINIK BIERECKI, CHRISTOPHE GAIE, MIROSŁAW KARPIUK

Artificial Intelligence in e-Administration

Abstract

Nowadays, the influence exerted by artificial intelligence on many spheres of human life has been steadily on the rise. It is a tool that e-Administration can – or should – use in its activities. However, caution must be exercised when using artificial intelligence systems, as their inappropriate use can lead to several threats, including data leakage or infection of the ICT systems through which the public administration provides its services to society or other entities (including entrepreneurs). Artificial intelligence is both a challenge and a necessity for public administration. With the development of new technologies, it must use modern tools to meet society's constantly evolving needs. Digitisation is now a widespread phenomenon, so meeting the needs of an information society forces public administration to look for new solutions, of which artificial intelligence is certainly one of these. The dogmatic-legal and theoretical-legal methods were employed to address the issues dealt with in the paper, which aims to analyse the need for e-Administration to use artificial intelligence. These methods have made it possible to review and analyse the applicable regulations and doctrinal views on the use of artificial intelligence systems by the public administration in the course of performing certain activities in cyberspace.

KEYWORDS: artificial intelligence, e-Administration, public sector, cybersecurity.

DOMINIK BIERECKI – associate professor, Pomeranian University in Słupsk (Poland), ORCID – 0000-0001-6993-3974, e-mail: dominik.bierecki@upsl.edu.pl
CHRISTOPHE GAIE – PhD in telecomunications, French Prime Minister Services (France), ORCID – 0000-0002-8252-5278, e-mail: christophe.gaie@gmail.com
MIROSŁAW KARPIUK – full professor, University of Warmia and Mazury in Olsztyn (Poland), ORCID – 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl

HTTPS://DOI.ORG/10.36128/PRIW.VI53.1201

1 Introduction

The recent surge of interest in artificial intelligence (AI) is the culmination of a long evolutionary process. It began with the pioneering work of Alan Turing,[1] where he presented nine arguments to demonstrate the possibility of machines exhibiting human-like intelligence. The history of AI is long and punctuated by periods of active research and development followed by periods of less progress, as described by Hoffman.[2] Recently, there has been a huge step in democratizing AI usage, largely attributed to the breakthrough of Generative AI.[3] Indeed, Generative AI has made AI accessible to a wider audience, even those without specialized technological knowledge. As a result, there are now millions of users and tens of millions of requests made to various AI tools, especially ChatGPT and Gemini.[4] This paper describes the factors that contribute to the emergence and adoption of AI-powered public services, as synthesized in Figure 1 thereafter.

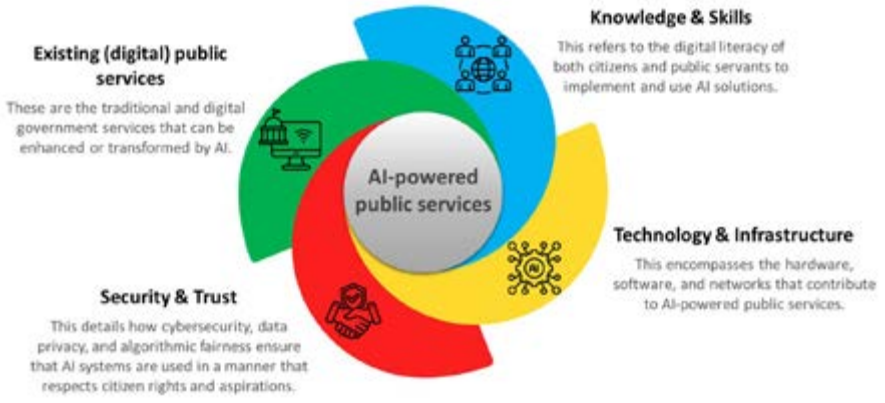

Figure 1: Factors that contribute to the emergence and adoption of AI-powered public services (template presentationgo.com, author: Dr. Christophe Gaie)

1 Alan Turing, "Computing machinery and intelligence" Mind 59, (1050): 433-460.

2 Christian Hugo Hoffmann, "Is AI intelligent? An assessment of artificial intelligence, 70 years after Turing" *Technology in Society*, Vol. LXVIII (2022): 101893. https://doi.org/10.1016/j.techsoc.2022.101893.

3 Adam Blandin, Alexander Bick, David Deming, *The Rapid Adoption of Generative* AI, 18 September 2024. https://ssrn.com/abstract=4965142 or http://dx.doi.org/10.2139/ssrn.4965142

4 Yan Liu, He Wang, *Who on Earth Is Using Generative AI?* (Washington, DC: World Bank, 2024). https://openknowledge.worldbank.org/server/api/core/bitstreams/9a202d4b-c765-4a85-8eda-add8c96df40a/content.

First, the rise of AI necessitates ensuring that both individuals and institutions are equipped to effectively and securely leverage these powerful tools. This is where digital literacy comes into play. Indeed artificial intelligence is best used in a digital state and society where both public institutions and their beneficiaries have adequate digital competencies which warrant the effective and secure use of new technologies, including artificial intelligence.

Digital accessibility and digital competencies are equally important. Digital accessibility, especially regarding public services, facilitates and accelerates contact between office staff and service recipients, making it possible to handle many affairs remotely, including for those who have difficulty reaching the office. Digital competencies enable the appropriate use of ICT tools, which are, these days, very much needed in various spheres of social and professional life. The development of new technologies makes the ability to use such tools indispensable, as they create opportunities for human development and determine progress in many spheres of human activity. Acquiring and expanding such competencies enables the optimal use of services provided in cyberspace and contributes to limiting digital exclusion[5].

Artificial intelligence can make access to services provided to society much easier. This will allow, on the one hand, to improve the operation of public administration and, on the other hand, raise living standards, making these services generally more accessible and, at the same time, cheaper. For example, it can help taxpayers at any time of the day to verify whether they are complying with fiscal legislation in a specific and complex situation. It can improve the quality of the response to a citizen who wants to obtain a public subsidy to initiate an ecological or social incentive. It can also help patients to accurately follow their medical treatment and react effectively in case of suspected side effects. For all these situations, it is noteworthy that AI transcends simple digitalization of public services. Moving beyond mere machine interactions may be considered as human-machine collaboration.[6]

While AI offers significant potential to improve public services, its effective and secure implementation is crucial. This necessitates a robust

5 Christophe Gaie, Mirosław Karpiuk, Andrea Spaziani, "Cybersecurity in France, Poland and Italy" *Studia Iuridica Lublinensia*, No. 1 (2025).

6 James Wilson, Paul Daugherty, "Collaborative intelligence: Humans and AI are joining forces" *Harvard Business Review*, 4 (2018): 114-123.

cybersecurity framework within the context of e-Administration. As e-Administration relies on ICT systems operating in cyberspace, these systems must be resilient to threats that could disrupt their functioning. Therefore, it appears of the utmost importance to ensure cybersecurity, which will guarantee these services are of an appropriate quality and can be delivered to recipients on time, especially against AI-specific vulnerabilities.[7] E-Administration operations must meet the appropriate standards to offer protection against cyber threats. Cybersecurity plays a crucial role in ensuring the threat resilience of artificial intelligence systems and in counteracting unauthorised modification or attempts to use such systems for illegal activities.

The objective of cybersecurity is to protect ICT systems against threats that disrupt their functioning.[8] These systems are widely used by the private sector and public administration alike. In the private sector, cybersecurity has a very high significance for financial entities. Under the Digital Operations Resilience Act (DORA, securing financial entities against threats resulting from the development of ICT systems shall be achieved by establishing uniform requirements for the security of networks and IT systems supporting the business processes of financial entities. The purpose of these requirements is to achieve a high and common level of

7 Viacheslav Moskalenko, Viacheslav Kharchenko, Alona Moskalenko, Boris Kuzikov, "Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods" *Algorithms*, 3 (2023): 165. https://doi.org/10.3390/a16030165.

8 For more information on the notion of cybersecurity, see also Christophe Gaie, Mirosław Karpiuk, "The Provision of e-Services by Public Administration Bodies and Their Cybersecurity", [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, ed. Christophe Gaie, Mayuri Mehta (Cham: Springer, 2024), 183-184; Małgorzata Czuryk, "Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 44-45; Zbigniew Nowak, "Agencja Cyberbezpieczeństwa – polska wersja The National Cyber Security Centre, Narodowego Centrum Cyberbezpieczeństwa Wielkiej Brytanii", [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. 25 lat członkostwa w NATO*, eds. Katarzyna Chałubińska-Jentkiewicz, Krzysztof Gawkowski, Zbigniew Nowak, Łukasz Piątkowski, Krzysztof Wąsik (Gliwice: Helion, 2024), 153-154; Mirosław Karpiuk, Jarosław Kostrubiec, "Provincial Governor as a Body Responsible for Combating State Security Threats" *Studia Iuridica Lublinensia*, No. 1 (2024): 117; Ewa Maria Włodyka, „Cyberbezpieczeństwo sektora publicznego", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warsaw: ASzWoj, 2024), 64; Sk Tahsin Hossain, Tan Yigitcanlar, Kien Nguyen,Yue Xu, „Cybersecurity in local governments: A systematic review and framework of key challenges" *Urban Governance* No. 1 (2025).

operational digital resilience.[9] As for the public administration, ICT systems facilitate using artificial intelligence to support carrying out tasks entrusted to it by the legislator. For example, cybersecurity plays a crucial role in facilitating the safe and effective use of AI by public administrations. This includes protecting AI models and training data by safeguarding sensitive information, preventing unauthorised access or manipulation, and ensuring the integrity of the training process. Furthermore, cybersecurity is essential for detecting and mitigating AI-powered threats, such as sophisticated malware and AI-driven phishing attacks, through the use of AI and machine learning techniques.

Ensuring the security of AI systems is also very important to avoid malicious use, notably informational attacks such as propaganda, data manipulation, or deepfakes.[10] Indeed, as disinformation is one of the specific threats caused by artificial intelligence, the integrity and authenticity of information sources appearing on the web should be protected and verified. Moreover, the indiscriminate use of modern digital tools should be avoided. The public sector should also conduct campaigns against disinformation, as it has an obligation not only to protect information and prevent its leakage, but also to counter the spread of false information, especially that which is of great importance to the state and its security.

2 The path from e-Government to AI-powered Government

To facilitate the adoption and development of AI-powered government services, the state should be involved in the development of information technologies within the public administration itself, in the domain of its interaction with citizens, and as part of the state's investment in

9 Dominik Bierecki, "Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operations Resilience Act)" *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, No. 3 (2024): 6.

10 Taís Fernanda Blauth, Oskar Josef Gstrein, Andrej Zwitter, "Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI" *IEEE Access*, Vol. X (2022): 77110-77122.

telecommunications infrastructure.[11] The development of these technologies also affects the functioning of public administration, which must be open to new phenomena, including artificial intelligence. Government services can foster e-Administration development in several ways. One approach is establishing e-Government platforms.[12] These software infrastructures enable the rapid creation of secure and user-friendly online portals for citizens to access government services. Examples include web portals like gov.uk (UK) and gouv.fr (France), along with open or protected development platforms like GitHub.[13] In the same vein, governments are also paying close attention to the development of interoperable services like Application Programming Interfaces (APIs) accessible through such portals as https://open.canada.ca (Canada), https://www.api.gov.uk/ (UK), or https://www.api.gouv.fr (France).[14] Indeed, interoperability will facilitate the transition from traditional digital services to innovative services that leverage AI to integrate and analyze multiple sources of information.[15]

Government initiatives to foster digital literacy programs are crucial for accelerating the emergence and adoption of AI services. By enhancing the digital skills of the population and cultivating a future IT workforce, these programs contribute to a more digitally proficient society. This, in turn, facilitates the development and effective utilization of digital services, as research has shown a strong correlation between higher levels of digital literacy and increased use of e-government services, improved user satisfaction, and greater civic participation.[16]

---

11 Dominik Tyrawa, "Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane" *International Journal of Legal Studies*, No. 1 (2023): 19.

12 Qi Min, Min Oi, Junshu Wang, "Using the Internet of Things E-Government Platform to Optimize the Administrative Management Mode" *Wireless Communications and Mobile Computing*" (2021).

13 Serhiy Shkarlet, Igor Oliychenko, Maksym Dubyna, Maryna Ditkovska, Vladimir Zhovtok, "Comparative analysis of best practices in e-Government implementation and use of this experience by developing countries" *Administratie si Management Public*, 34 (2020): 118-136.

14 Christophe Gaie, "An API-intermediation system to facilitate data circulation for public services: the French case study" *International Journal of Computational Systems Engineering*, 4 (2021): 201. 2

15 Yueshen Xu, Yinchen Wu, Honghao Gao, Shengli Song, Yuyu Yin, and Xichu Xiao, "Collaborative APIs recommendation for Artificial Intelligence of Things with information fusion" *Future Generation Computer System*, 125, C (2021): 471-479.

16 Abdulrazaq Kayode Abdulkareem, Kazeem Adebayo Oladimeji, "Cultivating the digital citizen: trust, digital literacy and e-government adoption" *Transforming Government: People, Process and Policy*, No. 2 (2024): 270-286.

Building public trust is crucial for the successful adoption and enhancement of digital government services with artificial intelligence. This requires a strong emphasis on cybersecurity that ensures the optimal functioning of e-Administration and requires observing cybersecurity rules and recommendations. Respecting them allows the safe use of artificial intelligence systems, which must be duly protected against unauthorised interference, thus continuously facilitating the provision of e-services of sufficient quality when using such systems. Addressing cybersecurity within e-government requires a multi-faceted approach. This includes identifying potential threats from various actors, including cybercriminals (often targeting financial gain), adversarial state actors, and terrorist groups (who may seek to spread misinformation or disrupt government services).[17] Furthermore, it is crucial to identify and mitigate specific attack vectors, such as worms, malware, distributed denial-of-service attacks, ransomware, and zero-day exploits. This can be facilitated by fulfilling the recommendations of the EBIOS method.[18] Finally, continuous monitoring and vulnerability management are paramount. This involves the constant monitoring of devices, software, and network traffic through dedicated security systems such as Endpoint Detection and Response (EDR) and its evolution, eXtended Detection and Response (XDR), to proactively identify and address security threats.[19]

The significance of cybersecurity to an information society extends beyond the technical aspects of ICT infrastructure and digital competencies. A holistic approach must also consider the broader security environment and the international landscape.[20] Given that artificial intelligence is deeply rooted in cyberspace, it can also be analysed (like cyberspace and cybersecurity) from different angles. Just as we must consider the security of the physical infrastructure that supports AI systems, we must

17 Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro, Cyber security: State of the art, challenges and future directions" *Cyber Security and Applications*, No. 2 (2024): 100031.

18 https://cyber.gouv.fr/publications/ebios-risk-manager-method.

19 George Shaji, George Hovan, Thangaraj Baskar, Digvijay Pandey, "XDR: The Evolution of Endpoint Security Solutions – Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future" *International Journal of Advanced Research in Science, Communication and Technology*, 1 (2021): 493-501.

20 Krzysztof Kaczmarek, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 105-106.

also consider the security of the data they process and the potential for AI itself to be used as a weapon.[21]

The proposed path towards the adoption of AI for e-Government is illustrated in Figure 2 below:

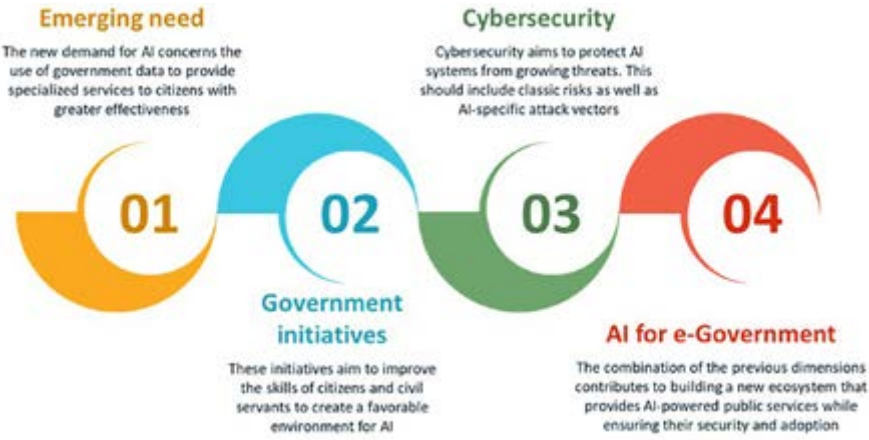

Figure 2: Proposed path towards the adoption of AI for e-Government (template presentationgo.com, author: Dr. Christophe Gaie)

The aim of this paper is to analyse the possibilities of using artificial intelligence systems in e-government. The basic research method to pursue the set objective is the formal-dogmatic method. It was employed to analyse the legal regulations governing the status of e-Administration, as well as the opportunities for it to use artificial intelligence. The theoretical-legal method was also used to present the views of the doctrine on artificial intelligence and related concepts.

21 Muhammad Mudassar Yamin, Mohib Ullah, Habib Ullah, Basel Katt, "Weaponized AI for cyberattacks" *Journal of Information Security and Applications*, Vol. LVII (2021): 102722.

3 The use of artificial intelligence in e-Administration

3.1. Definition and Scope of Artificial Intelligence and e-Administration

The term "artificial intelligence" covers diverse types of software or hardware components supporting machine learning, computer vision, natural language understanding, generation and processing, as well as robotics. Artificial intelligence enables machines to collect and analyse information about their surroundings and to act to achieve a specific objective. Based on observation and experience, some artificial intelligence systems are capable of adapting their behaviour patterns to their surroundings and acting autonomously.[22] According to the legal definition, artificial intelligence means a machine system which (1) is designed to operate with varying levels of autonomy once deployed, (2) can display adaptability once deployed, and (3) is capable of inferring (for explicit or implicit purposes) how to generate results that can influence the physical or virtual environment, based on the input data received.[23]

The field of artificial intelligence provides exciting opportunities and significant challenges. It has great potential to revolutionise the way public services are delivered. Indeed, AI can improve interactivity between citizens and government services, automate various processes for greater efficiency, or propose predictive analytics to facilitate the work of civil servants. As AI tends to replace human processes, it's crucial to address the ethical considerations, ensure transparency, and maintain public trust to ensure the fundamental rights of citizens.

The term "e-Administration" (or e-Government) refers to the "use of ICTs to more effectively and efficiently deliver government services to citizens

22 Krzysztof Kaczmarek, „Sztuczna inteligencja", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warsaw: ASzWoj, 2024), 251-252.

23 Article 3 (1) of the Regulation of the European Parliament and of the Council (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)) (OJ EU L 2024/1689).

and businesses", as defined by the United Nations.[24] It covers a wide range of activities, from providing online access to information and services, such as applying for a driver's license or paying taxes, to using technology to improve internal government operations, such as data analysis for policy-making and digital communication within government agencies.

As described in the authors' previous work,[25] e-Administration modernizes government by streamlining processes, improving service delivery, and increasing citizen engagement. It focuses on online access to information and services, mobile accessibility, open data, and digital inclusion. Successful implementation requires strong strategies, robust infrastructure, human resource development, and collaboration. Benefits include improved service delivery, increased transparency and accountability, enhanced citizen participation, and economic growth.

3.2. Accelerating the growth of e-Administration with Artificial Intelligence

E-Administration uses information technology in the performance of the state's administration tasks. In a narrow sense, this is an electronic information system, a set of administrative services and processes offered by the public administration. In a broader sense, attention is drawn to the trend of adopting innovative approaches to public policy-making. The notion of e-Administration should be combined with notions such as standardisation, digitisation and computerisation on the one hand and the increasing attention to cybersecurity issues in the public sector on the other. The aim is to optimise state management processes and to serve citizens.[26] E-Administration is an organisation that should be knowledge-based and

24 UN. (2023). Overview of e-Government. United Nations. https://publicadministration.un.org/ egovkb/en-us/Overview.

25 Christophe Gaie, Mayuri Mehta, "Digital Transformation of Public Services: Introduction, Current Trends and Future Directions", [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, ed. Christophe Gaie, Mayuri Mehta (Cham: Springer, 2024), 175-188.

26 Ewa Maria Włodyka, „E-administracja", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warszawa: ASzWoj, 2024), 118; See also Kaisu Sahamies, Olga Welinder, „Orchestrating Sustainability: Government Platforms for Material Circulation" *Administration and Society*, No. 1 (2025): 101.

should use ICT systems to carry out public tasks. In addition, it should be innovative and thus open to new technologies, with employees displaying a high level of digital competencies.

The mission of public sector institutions is to effectively address society's needs. They increasingly perform the tasks assigned to them using ICT systems, which both improve the performance of public tasks and allow them to reduce their costs or reach a wider audience in a relatively short period. The public sector is a factor stimulating the process of providing social services, as well as enforcing specific behaviours of the participants in the process.[27] The provision of public e-services can be supported by artificial intelligence, which should contribute to their optimisation in terms of quality, availability and time of service provision.

Following a sustained period of digital service adoption, it is now crucial to ensure that public services are easily accessible to low-skilled citizens. Artificial intelligence can significantly assist by identifying poorly formulated requests and suggesting corrections, enabling citizens to achieve their goals with minimal effort. Furthermore, AI can proactively suggest actions to ensure legal compliance and optimize citizens' behaviour.[28] For instance, it may alert them to a significant change in income between consecutive years, which may indicate a potential fraud risk. Additionally, AI can automate the preparation of grant subsidy claims, streamlining processes such as those involved in recognizing a new child.

A key dimension for implementing AI in public services relies on the new potential for improvement for civil servants. Indeed, the introduction of AI in their daily work enables them to benefit from new abilities that optimize their activity. Among the infinite possibilities of application, there are basic usages such as speech-to-text, language translation, redacting meeting minutes, proposing answers to citizens' questions, etc. AI can also provide support for more complex tasks such as identifying potential frauds, optimizing healthcare resource allocation, optimizing agriculture subsidy distribution, detecting cybersecurity attacks, etc.

27 Mirosław Karpiuk, Claudio Melchior, Urszula Soler, "Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 8.

28 Samuel Dike, "The Role of Artificial Intelligence and Research in Promoting Taxpayer Base and Behaviour" *The International Journal of Social Sciences and Humanities Invention*, No. 11 (2020).

3.3. Implementing AI in e-Administration: Policy, Legislation and Challenges

3.3.1. Defining a policy for implementing AI-powered public services

The policy on artificial intelligence assumes that the solutions adopted in this field are expected to improve the efficiency of government and local government administration, and the continuous expansion of technical capabilities makes process automation increasingly attractive for public administration. Thanks to advances in artificial intelligence, processes that a few years ago had to be carried out by many civil servants can today be at least partially automated. However, it should be emphasised that the task of this administration should be to set standards for the implementation of artificial intelligence solutions, in particular, to ensure respect for ethics, protect citizens' rights and improve the quality of public services offered.[29] In the case of the implementation of artificial intelligence tools, it must, therefore, be ensured, *inter alia*, that human freedoms and rights are adequately protected. Restrictions on the exercise of constitutional freedoms and rights must not lead to a violation of human dignity. Drastic restrictions that will be disproportionate to the objective to be achieved through them may lead to a violation of human dignity, with each case of restriction of individual freedoms and rights to be treated on a case-by-case basis, taking into account the circumstances in each case.[30]

Poland's policy for the development of artificial intelligence has the following objectives: 1) to effectively coordinate all activities related to developing the Polish artificial intelligence system; 2) to establish rules of transparency, auditing and accountability for the use of algorithms by public administration, which includes introducing mandatory self-assessment defining the problem and sharing responsibility for the system's operation, potential errors and undertaken remedial measures, and to develop a model explanation of decisions taken with the support of artificial intelligence

29 *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020* (Warsaw: KPRM, 2020), 67.

30 Małgorzata Czuryk, "Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 32. See also: Jarosław Kostrubiec, *Sztuczna inteligencja a prawa i wolności człowieka* (Warsaw: IWS, 2021): 21; Małgorzata Czuryk, "Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd" *Studia z Prawa Wyznaniowego*, No. 27 (2024): 158.

and the possibility of appealing against such decisions, in particular if they directly influence individual rights and freedoms; 3) to increase the state's capacity to use artificial intelligence in case of emergency, in order to project risks and support decision-making, as well as in situations requiring intervention or support from public administration (central and local); 4) to use solutions specific to artificial intelligence for the continuous monitoring and improvement of the natural environment; 5) to use the potential of artificial intelligence in the medical sphere to improve the health of citizens, taking into consideration the issues of privacy and personal data protection; and 6) to increase the procurement of artificial intelligence systems in the public sector, including the procurement by government administration, self-government bodies, state-owned companies and municipal companies of local government units.[31]

In the case of using artificial intelligence systems by e-Administration, it must have suitably qualified staff who, on the one hand, know how to use such tools and, on the other, know how to do so safely without causing threats to the institution they represent, to themselves or to the persons using the services provided using artificial intelligence.

3.3.2. Complying with European regulations for the implementation of AI in public administrations

The EU legislator, in Article 4 of the Artificial Intelligence Act, makes it clear that entities using artificial intelligence systems are required to take measures to ensure, as far as possible, an adequate level of artificial intelligence competencies among their staff and other persons involved in operating and using such systems on their behalf. In doing so, the technical knowledge, experience, education or training of such staff and persons should be taken into account, as well as the application context and people (or groups of people) concerning whom these artificial intelligence systems are planned to be used. The principle of article 4 of the Artificial Intelligence Act should be considered while applying all kinds of duties of this regulation. This is a meta-norm that is an implementation in the Artificial

31 *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020* (Warsaw: KPRM, 2020), 69-71.

Intelligence Act of the principle of proportionality manifested in Article 5, Paragraph 4 of the Treaty on European Union.[32]

For high-risk artificial intelligence systems, the legislature requires the implementation of a risk management system. A risk management system, as defined in Article 9 (2) of the Artificial Intelligence Act, is understood as a continuous and recurrent process, both planned and implemented throughout the life cycle of a high-risk artificial intelligence system, requiring regular reviews and updating. Typically, the following variants of handling risks are distinguished: 1) acceptance, 2) reduction, 3) retention, 4) sharing, 5) avoidance, and 6) transfer. The final stage of the risk management process should be to verify the effectiveness of solutions implemented in this regard.[33] In the case of high-risk management systems, human oversight should be assured. Those systems should be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use. Again, the principle of proportionality manifest itself in the article 14 paragraph 3 of the Artificial Intelligence Act. According to the provision of this article, the oversight measures shall be commensurate with the risks, level of autonomy and the context of use of the high-risk AI system.

Article 5 (1) of the Artificial Intelligence Act prohibits the marketing, commissioning or use of an artificial intelligence system that employs subliminal techniques which are beyond the person's awareness or deliberate manipulative or deceptive techniques which have the purpose or effect of significantly altering the behaviour of a person (or group of people) by materially impairing their ability to make informed decisions that are likely to cause serious harm. Such practices cannot be used by e-Administration.

32 On the principle of proportionality in the EU law see: Justyna Maliszewska-Nienartowicz, *Zasada proporcjonalności jako podstawa oceny legalności ograniczeń swobód rynku wewnętrznego Unii Europejskiej* (Toruń: Wydawnictwo Naukowe UMK: 2020), 77-84.

33 Filip Radoniewicz, "Zarządzanie ryzykiem", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warsaw: ASzWoj, 2024), 293.

3.3.3. Identifying and addressing the challenges for the implementation of AI in public administrations

The successful implementation of AI in e-Administration necessitates careful consideration of several limitations and challenges. These includes preventing bias, ensuring a high level of data diversity and quality, utilizing fair AI algorithms, guaranteeing human oversight, and fulfilling ethical considerations.

Figure 3: Five challenges to implement Artificial Intelligence to achieve e-Administration (template presentationgo.com, author: Dr. Christophe Gaie)

As a matter of fact, the introduction of AI in public services may create biases that engender prejudice against certain individuals or groups. This can manifest in various ways, such as lower recruitment prospects, a higher probability of police control, erroneous ethnic assumptions in medical treatment, and other discriminatory outcomes.

AI biases can arise from various factors. One significant contributor is the limitations of the datasets used to train these systems. For example, if a dataset underrepresents certain groups, like women in leadership positions, the AI may learn and perpetuate these existing biases[34]. This can

34 Erini Ntoutsi, Pavlos Fafalios, et al. Bias in data-driven artificial intelligence systems – An introductory survey. WIREs Data Mining Knowl Discov. 2020; 10:e1356. https://doi.org/10.1002/widm.1356.

lead to discriminatory outcomes in areas like recruitment, where the AI might unfairly favour male candidates. Another example of potential bias stems from energy policies that tend to maintain high levels of subsidies for industrial services while neglecting the promotion of renewable energies.

Algorithms used by AI systems are also a significant source of bias. These algorithms may rely heavily on general statistical trends while insufficiently considering the unique circumstances of individual cases. For example, algorithms might overestimate the likelihood of a criminal re-offending[35] by failing to adequately account for crucial reintegration factors such as securing employment, raising children, diligently adhering to therapy, or complying with electronic monitoring. Another concerning example involves AI systems used to enhance education.[36] In lower-income communities, the algorithm might suggest overly simplistic exercises for high-achieving students, potentially hindering their intellectual growth and contributing to social disadvantage. In this scenario, AI could inadvertently exacerbate existing disparities rather than mitigate them.

To ensure the adequate usage of AI systems, the literature emphasizes the importance of developing and employing fair algorithms. These computational programs should adhere to stringent requirements in terms of transparency, explainability, and mitigation of discrimination risks. For example, determining eligibility for a social welfare program like housing assistance should rely on a transparent decision-making process with clear criteria such as income, family size, and employment history being explicitly weighted. Over-reliance on a single criterion can create a feedback loop and potentially exacerbate existing biases.[37] Moreover, the steps of the decision-making process should be explainable so that a citizen can understand the reasons for the denial of their request and has the possibility to obtain a human review to guarantee a fair examination of their situation. Finally, the algorithm should be rigorously tested to ensure that it does not disproportionately favor applicants with certain characteristics, such as those from specific neighborhoods or with certain ethnic backgrounds.

35 Heeket Mehta, Shanay Shah, Neil Patel, Pratik Kanani, "Classification of criminal recidivism using machine learning techniques" *International Journal of Advanced Science and Technology*, No. 4 (2020): 5110-5122.

36 Ryan Baker, Aaron Hawn, "Algorithmic Bias in Education" *International Journal of Artificial Intelligence in Education*, 32 (2022): 1052-1092.

37 Bo Cowgill, Catherine Tucker, "Economics, fairness and algorithmic bias" *Journal of Economic Perspectives*, (2019).

A very important dimension to provide trust in AI is the guarantee of human oversight in the decision process so that control is ensured throughout the process. To this end, it is recommended to establish human-in-the-loop systems. This is achieved by incorporating human oversight and intervention mechanisms at different stages of the process to review and correct potentially erroneous decisions made by AI systems.[38] For example, the detection of a cybersecurity threat should be reviewed by a cyber specialist to avoid automatic blockage of flows that could paralyze the IT system in case of error.

While human oversight is essential to reduce bias and ensure responsible use of AI in public services, implementing it comes with its own hurdles. We need to carefully consider factors like cost, expertise needed, and potential delays in decision-making. Assigning oversight roles requires finding qualified people who understand both the specific AI system and the area it's used in (e.g., healthcare, social services). Additionally, adding human review processes can make things more complex and potentially slow down decision-making. Establishing the right balance between human oversight and efficiency is key to maximizing the benefits of AI in government.[39]

To address these challenges, establishing clear procedures can help make human oversight more effective.[40] These procedures should respect human judgment (discretion), ensure fairness (proportionality), and consider the non-technical impacts of decisions. This awareness ensures that human intervention adds clear value by safeguarding the organization's strategic goals. For example, an AI system might suggest a specific aggressive treatment plan based on a patient's risk profile. However, the physician should review this recommendation, considering the patient's age, overall health, and personal preferences. This ensures that the treatment plan aligns with the patient's individual needs and values, and does not unnecessarily disrupt their quality of life.

A major concern for the adoption of AI in the context of e-government is the fulfilment of ethical considerations. As discussed previously, the

38 Rohani Rohan, Suree Funilkul, Debajyoti Pal and Himanshu Thapliyal, Humans in the Loop: Cybersecurity Aspects in the Consumer IoT Context" *IEEE Consumer Electronics Magazine*, No. 4 (2022): 78-84.

39 Madalina Busuioc, "Accountable Artificial Intelligence: Holding Algorithms to Account" *Public Administration Review*, 81 (2021): 825-836.

40 Riikka Koulu, "Proceduralizing control and discretion: Human oversight in artificial intelligence policy" *Maastricht Journal of European and Comparative Law*, 6 (2020): 720-735.

transparency and explainability are crucial to provide citizens with access to information about the data and algorithms used in AI systems as well as the saving of their own queries. Indeed, the use of AI systems in government raises important privacy concerns as governments need to ensure that AI systems are designed and used in a way that protects the privacy of citizens[41]. This may involve developing data minimization techniques and strong data security measures.

Ensuring ethical considerations are respected requires clearly defined lines of accountability for developing and deploying AI systems in government. This means that everyone involved understands who is responsible for ensuring the ethical and responsible use of AI. Accountability is particularly important in the public sector, where AI algorithms are increasingly used for high-stakes decisions. Interesting proposals include requiring greater transparency from AI developers. This could involve requiring developers to disclose how their algorithms work and how the data they are trained on. Additionally, developing new standards for algorithmic fairness could help ensure that AI algorithms are not biased against certain groups of people.

Furthermore, considering the potential social, economic, and environmental impacts of AI systems is crucial. Implementing AI in public systems and adapting to new possibilities for faster, higher-quality work can be challenging for some civil servants. Citizens, too, should be reassured about the technology's mastery, ethical use, and the ability to explain decisions, hold actors accountable, maintain human oversight, and avoid bias. For instance, France has defined a comprehensive AI strategy to achieve these goals[42] and promotes experimentation to reach them. For example, France's current experiment with Albert, an open source solution developed entirely in-house, guarantees the French administration total control over the data exchanged and strengthens the country's digital sovereignty.[43]

In the case of artificial intelligence, there are a large number of tools that can be used to have both positive and negative effects on society.

41 Omar Saeed Al-Mushayt, "Automating E-Government Services With Artificial Intelligence" *IEEE Access*, Vol. VII (2019): 146821-146829.

42 French Artificial Intelligence Commission. (2024). Ai: Our Ambition For France. https://www.info.gouv.fr/upload/media/content/0001/10/54eefd62c084d-66c373a8db1eefaeed88a21b010.pdf.

43 Émeline Cirou, "Say hello to Albert! The new AI in French public services" *Blog Economie Numérique*, 2024. https://blog.economie-numerique.net/2024/05/06/say-hello-to-albert-the-new-ai-in-french-public-service/.

Considering the risks, the main drawback of artificial intelligence is that it can be used to conduct an effective disinformation process. This is because artificial intelligence can manipulate the public, including through fake news and information noise.[44]

A public entity is obliged to use only those ICT systems which meet the relevant requirements and ensure their interoperability for the performance of public tasks.[45] ICT systems used by entities fulfilling public tasks are designed, implemented and operated by taking into consideration their functionality, reliability, usability or efficiency, as well as by applying the appropriate norms and professionally recognised standards and methodologies.[46] Only such systems will allow e-Administration to properly use artificial intelligence in the public domain.

4 Conclusion

Artificial intelligence is a tool most readily used in information society, which is defined as a technologically advanced society where national income is based on information processing, which is the source of maintenance for

44 Tomasz Gergelewicz, "Bipolarity of Artificial Intelligence – Chances and Threats" *Ius et Securitas* No. 2 (2024). For more details on disinformation, see also Justyna Olędzka, „Zjawisko dezinformacji jako źródło zagrożeń bezpieczeństwa państwa – zarys problematyki", [in:] *Współczesne zagrożenia bezpieczeństwa*, ed. Adam Jelonek (Warsaw: ASzWoj, 2024); Tomasz Gergelewicz, *Informacja sygnalna. Katalog obszarów działań antydezinformacyjnych* (Warsaw: ASzWoj, 2023); Krzysztof Kaczmarek, "Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych" *Rocznik Nauk Społecznych* No. 2 (2023); Piotr Dzikowski, „Propaganda, plotka, dezinformacja – czy to działa tylko na zewnątrz organizacji?", [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. Paweł Dziuba (Warsaw: WAT, 2023); Maciej Ciesielski, „Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities" *Cybersecurity and Law*, No. 1 (2024).

45 Article 13 (1) of the Act o 17 February 2005 on Computerisation of the Activities of Entities Carrying out Public Tasks (consolidated text, Journal of Laws of 2024, item 1557 as amended).

46 § 15 (1) of the Regulation of the Council of Ministers of 21 May 2024 on the National Interoperability Framework, minimum requirements for public registers and the exchange of information in electronic form and minimum requirements for information and communication systems (Journal of Laws of 2024, item 773).

the majority of its members.[47] The successful implementation of AI in e-Administration requires to addressing several challenges. As described in this article, this include mitigating bias in AI algorithms, ensuring data quality and diversity, and establishing clear lines of accountability. Moreover, human oversight remains crucial throughout the decision-making process to guarantee fairness and responsible use of AI.

In the era of information society and the digital state, where universal access to electronic services is taken for granted, cybersecurity becomes particularly important, as it not only enables uninterrupted social communication but allows strategic sectors of the economy to function properly. As cybersecurity offers protection against threats, it also ensures the appropriate operation of the state as a public entity at many levels.[48]

Disruptions in cyberspace can have a negative impact on society as well as on the functioning of the state, which has to ensure an appropriate quality of its services, including those of strategic importance. Given the need to adequately secure such services and to ensure their continuity and availability, it is necessary to take measures to secure them.[49]

To use AI tools effectively, digital literacy needs to be enhanced, both in society and in public administration, which should use AI to perform public tasks. In addition, public administration must be open to cooperation with the private sector, which is more responsive to changes in new technologies, with the scientific sector and with social organisations representing potential recipients of public e-services.

Attention should also be paid to the legal and ethical context of artificial intelligence. It is particularly important to protect personal data and intellectual property, to recognise responsibility for the damage caused by artificial intelligence systems (whether by the developers, operators or end users) or to safeguard legally protected secrets. Appropriate ethical standards must also be observed when using artificial intelligence tools, and attention must be paid to human and civil freedoms and rights – in particular, to human dignity. In addition, the international or technical context of artificial intelligence must not be underestimated. International

47 Filip Radoniewicz, "Społeczeństwo informacyjne", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warsaw: ASzWoj, 2024), 234.

48 Mirosław Karpiuk, „The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 190.

49 Mirosław Karpiuk, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022): 167-168.

legal solutions must consider the global aspect of artificial intelligence and protect the international community against the negative consequences of abusing artificial intelligence. International cooperation focused on implementing and assessing artificial intelligence systems and exchanging experience in this field is also important. At the same time, it is essential to prevent unauthorised restriction of access to artificial intelligence – whether countrywide, EU-wide or globally – and to promote fair market competition in new technologies, including artificial intelligence systems. Finally, the technically safe use of artificial intelligence systems should be promoted or even required, on condition that these systems are immune to disruptive threats, to ensure compliance with the relevant technical standards.

The risk of the emerging threats associated with artificial intelligence relates to both the design of such systems and their use. Due diligence must be exercised at both these stages to minimise threats as much as possible. Future research should focus on developing practical guidelines and best practices for reinforcing security in AI systems, a crucial element for the successful development of e-Administration. This approach will facilitate the creation and adoption of AI in e-Administration, leading to more equitable and efficient public services.

Bibliography

Abdulkareem Abdulrazaq Kayode, Kazeem Adebayo Oladimeji, "Cultivating the digital citizen: trust, digital literacy and e-government adoption" *Transforming Government: People, Process and Policy*, No. 2 (2024): 270-286. https://doi.org/10.1108/TG-11-2023-0196.

Admass Wasyihun Sema, Yirga Yayeh Munaye, Abebe Abeshu Diro, "Cyber security: State of the art, challenges and future directions" *Cyber Security and Applications*, No. 2 (2024): 100031. https://doi.org/10.1016/j.csa.2023.100031.

Al-Mushayt Omar Saeed, "Automating E-Government Services With Artificial Intelligence" *IEEE Access*, Vol. VII (2019): 146821-146829. doi: 10.1109/ACCESS.2019.2946204.

Baker Ryan, Aaron Hawn, "Algorithmic Bias in Education" *International Journal of Artificial Intelligence in Education*, 32 (2022): 1052-1092. https://doi.org/10.1007/s40593-021-00285-9.

Bierecki Dominik, "Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operations Resilience Act)" *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, No. 3 (2024): 5-13. https://doi.org/10.52097/eppism.9272.

Blandin Adam, Alexander Bick, David Deming, *The Rapid Adoption of Generative AI*, 18 September 2024. https://ssrn.com/abstract=4965142; http://dx.doi.org/10.2139/ssrn.4965142.

Blauth Taís Fernanda, Oskar Josef Gstrein, Andrej Zwitter, "Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI" *IEEE Access*, Vol. 10 (2022): 77110-77122. doi: 10.1109/ACCESS.2022.3191790.

Busuioc Madalina, "Accountable Artificial Intelligence: Holding Algorithms to Account" *Public Administration Review*, 81 (2021): 825-836. https://doi.org/10.1111/puar.13293.

Ciesielski Maciej, "Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities" *Cybersecurity and Law*, No. 1 (2024): 185-199.

Cowgill Bo, Catherine Tucker, "Economics, fairness and algorithmic bias" *Journal of Economic Perspectives*, (2019).

Czuryk Małgorzata, "Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52.

Czuryk Małgorzata, "Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd" *Studia z Prawa Wyznaniowego*, No. 27 (2024): 151-163.

Czuryk Małgorzata, "Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 31-43.

Dike Samuel, "The Role of Artificial Intelligence and Research in Promoting Taxpayer Base and Behaviour" *The International Journal of Social Sciences and Humanities Invention*, No. 11 (2020). http://dx.doi.org/10.21107/infestasi.v20i1.25002.

Dzikowski Piotr, „Propaganda, plotka, dezinformacja – czy to działa tylko na zewnątrz organizacji?", [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. Paweł Dziuba. 9-25.Warsaw: WAT, 2023.

Émeline Cirou, "Say hello to Albert! The new AI in French public services" *Blog Economie Numérique*, 2024. https://blog.economie-numerique.net/2024/05/06/say-hello-to-albert-the-new-ai-in-french-public-service/.

Gaie Christophe, "An API-intermediation system to facilitate data circulation for public services: the French case study" *International Journal of Computational Systems Engineering*, 4 (2011): 201. https://doi.org/10.1504/ijcsyse.2021.120292.

Gaie Christophe, Mirosław Karpiuk, "The Provision of e-Services by Public Administration Bodies and Their Cybersecurity", [in:] Transforming Public

Services – Combining Data and Algorithms to Fulfil Citizen's Expectations, ed. Christophe Gaie, Mayuri Mehta. 175-188. Cham: Springer, 2024.

Gaie Christophe, Mirosław Karpiuk, Andrea Spaziani, "Cybersecurity in France, Poland and Italy" *Studia Iuridica Lublinensia*, No. 1 (2025).

Gaie Christophe, Mayuri Mehta, "Digital Transformation of Public Services: Introduction, Current Trends and Future Directions", [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, ed. Christophe Gaie, Mayuri Mehta. 175-188. Cham: Springer, 2024. https://doi.org/10.1007/978-3-031-55575-6_1.

Gergelewicz Tomasz, "Bipolarity of Artificial Intelligence – Chances and Threats" *Ius et Securitas*, No. 2 (2024).

Gergelewicz Tomasz, Informacja sygnalna. Katalog obszarów działań antydezinformacyjnych (Warsaw: ASzWoj, 2023).

Hoffmann Christian Hugo, "Is AI intelligent? An assessment of artificial intelligence, 70 years after Turing" *Technology in Society*, Vol. LXVIII (2022): 101893, https://doi.org/10.1016/j.techsoc.2022.101893.

Hossain Sk Tahsin, Tan Yigitcanlar, Kien Nguyen, Yue Xu, „Cybersecurity in local governments: A systematic review and framework of key challenges" *Urban* Governance, No. 1 (2025).

Kaczmarek Krzysztof, „Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych" *Rocznik Nauk Społecznych*, No. 2 (2023): 19-30.

Kaczmarek Krzysztof, „Sztuczna inteligencja", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 250-252. Warsaw: ASzWoj, 2024.

Kaczmarek Krzysztof, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 103-121.

Karpiuk Mirosław, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022): 166-179.

Karpiuk Mirosław, „The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 189-201.

Karpiuk Mirosław, Claudio Melchior, Urszula Soler, "Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 7-27.

Karpiuk Mirosław, Jarosław Kostrubiec, "Provincial Governor as a Body Responsible for Combating State Security Threats" *Studia Iuridica Lublinensia*, No. 1 (2024): 107-122.

Kostrubiec Jarosław, *Sztuczna inteligencja a prawa i wolności człowieka*. Warsaw: IWS, 2021.

Koulu Riikka, "Proceduralizing control and discretion: Human oversight in artificial intelligence policy" *Maastricht Journal of European and Comparative Law*, 6 (2020): 720-735. https://doi.org/10.1177/1023263X20978649.

Liu Yan, He Wang, *Who on Earth Is Using Generative AI?*. Washington, DC: World Bank, 2024. https://openknowledge.worldbank.org/server/api/core/bitstreams/9a202d4b-c765-4a85-8eda-add8c96df40a/content.

Maliszewska-Nienartowicz Justyna, *Zasada proporcjonalności jako podstawa oceny legalności ograniczeń swobód rynku wewnętrznego Unii Europejskiej*. Toruń: Wydawnictwo Naukowe UMK: 2020.

Mehta Heeket, Shanay Shah, Neil Patel, Patrik Kanani, "Classification of criminal recidivism using machine learning techniques" *International Journal of Advanced Science and Technology*, No. 4 (2020): 5110-5122.

Min Oi, Junshu Wang, "Using the Internet of Things E-Government Platform to Optimize the Administrative Management Mode" *Wireless Communications and Mobile Computing*" (2021). https://doi.org/10.1155/2021/2224957.

Moskalenko Viacheslav, Viacheslav Kharchenko, Alona Moskalenko, Boris Kuzikov, "Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods" *Algorithms*, 3 (2023): 165. https://doi.org/10.3390/a16030165.

Nowak Zbigniew, "Agencja Cyberbezpieczeństwa – polska wersja The National Cyber Security Centre, Narodowego Centrum Cyberbezpieczeństwa Wielkiej Brytanii", [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. 25 lat członkostwa w NATO*, ed. Katarzyna Chałubińska-Jentkiewicz, Krzysztof Gawkowski, Zbigniew Nowak, Łukasz Piątkowski, Krzysztof Wąsik. Gliwice: Helion, 2024.

Ntoutsi Erini, Pavlos Fafalios, et al. "Bias in data-driven artificial intelligence systems – An introductory survey" *WIREs Data Mining and Knowledge Discovery*, (2020). https://doi.org/10.1002/widm.1356.

Olędzka Justyna, „Zjawisko dezinformacji jako źródło zagrożeń bezpieczeństwa państwa – zarys problematyki", [in:] *Współczesne zagrożenia bezpieczeństwa*, ed. Adam Jelonek. 109-118. Warsaw: ASzWoj, 2024.

Radoniewicz Filip, "Społeczeństwo informacyjne", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 233-234. Warsaw: ASzWoj, 2024.

Radoniewicz Filip, "Zarządzanie ryzykiem", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 290-293. Warsaw: ASzWoj, 2024.

Rohan Rohani, Suree Funilkul, Debajyoti Pal, Himanshu Thapliyal, "Humans in the Loop: Cybersecurity Aspects in the Consumer IoT Context" *IEEE Consumer Electronics Magazine*, No. 4 (2022): 78-84. doi: 10.1109/MCE.2021.3095385.

Sahamies Kaisu, Olga Welinder, "Orchestrating Sustainability: Government Platforms for Material Circulation" *Administration and Society*, No. 1 (2025): 100-128.

Shaji George, George Hovan, Thangaraj Baskar, Digvijay Pandey, "XDR: The Evolution of Endpoint Security Solutions – Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future" *International Journal of Advanced Research in Science, Communication and Technology*, 1 (2021): 493-501. https://doi.org/10.5281/zenodo.7028219.

Shkarlet Serhiy, Igor Oliychenko, Maksym Dubyna, Maryna Ditkovska, Vladimir Zhovtok, "Comparative analysis of best practices in e-Government implementation and use of this experience by developing countries" *Administratie si Management Public*, 34 (2020): 118-136. doi: 10.24818/amp/2020.34-07.

Turing Alan, "Computing machinery and intelligence" *Mind*, 59 (1950): 433-460.

Tyrawa Dominik, "Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane" *International Journal of Legal Studies*, No. 1 (2023): 13-30.

Wilson James, Paul Daugherty, "Collaborative intelligence: Humans and AI are joining forces" *Harvard Business Review*, 4 (2018): 114-123.

Włodyka Ewa Maria, "Cyberbezpieczeństwo sektora publicznego", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 64-67. Warsaw: ASzWoj, 2024.

Włodyka Ewa Maria, „E-administracja", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz. 112-119. Warszawa: ASzWoj, 2024.

Xu Yueshen, Yinchen Wu, Honghao Gao, Shengli Song, Yuyu Yin, Xichu Xiao, "Collaborative APIs recommendation for Artificial Intelligence of Things with information fusion" *Future Generation Computer System*, 125, C (2021): 471-479. https://doi.org/10.1016/j.future.2021.07.004.

Yamin Muhammad Mudassar, Mohib Ullah, Habib Ullah, Basel Katt, "Weaponized AI for cyber attacks" *Journal of Information Security and Applications*, Vol. LVII (2021): 102722. https://doi.org/10.1016/j.jisa.2020.102722.