GIS Odyssey Journal

2024 • Volume 4 • Number 2

https://doi.org/10.57599/gisoj.2024.4.2.165

Grażyna Szpor[1]

PLANNING THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS

Abstract: AI has already been the subject of multi-level legislation worldwide for several years. The year 2024 started the adoption phase of comprehensive, universally applicable acts worldwide. In the EU, the main such act is a regulation of the European Parliament and the Council – the AI Act. It contains dozens of definitions, which is beneficial for further lawmaking and application, also in the field of GIS systems. However, development plans do not cease to be important acts. The structural elements of AI development strategies are similar, but the motivations for developing these acts vary across countries. Research into the determinants of their greater or lesser effectiveness is useful in the creation and evaluation of drafts of new prospective acts. Relating them to the EU and Poland, it is possible to state both the diagnosis of shortcomings and attempts to reduce them in successive AI development plans, as well as the inclusion of the development of AI systems in comprehensive digital transformation strategies. The current economic potential of AI is assessed differently but risks associated with its development are not disputed. Therefore, it is necessary to prioritise maximising the effectiveness of cyber-security mechanisms in forming AI development policies.

Keywords: artificial intelligence system, AI, EU, digital transformation, cybersecurity

Received: 16 November 2024; accepted: 20 December 2024

[1] Cardinal Stefan Wyszyński University in Warsaw, Poland ORCID ID: 0000-0002-3264-9360, email: g.szpor@uksw.edu.pl

Introduction

The functioning of information systems is changing as a result of technological advances. The creation and use of information systems, including geographic information systems (GIS) is subject to multi-level regulation, which has been evolving for a decade to meet the new challenges of the rapid development of artificial intelligence systems (Global Views on A.I., 2023; Digital Poland, 2023; Gen AI, 2024).

The purpose of this article is to analyze "the prospective acts" (strategies, plans) of artificial intelligence (AI). It characterizes the new legal definitions of AI systems in the European Union, global regulatory trends and leaders of AI juridization. Planning for AI development in the EU was compared with previously initiated planning in authoritarian states. The policy of AI development in Poland as an exemplary EU member state is presented, paying attention to barriers to effectiveness.

Material and methods

The article presents the results of a desk research study of the strategies for the development of artificial intelligence. Legal acts, official documents, expert reports and scientific studies were analysed. Using legal research methods, the solutions adopted in the European Union and in Poland were evaluated against the background of solutions identified as models and those occurring in other countries advanced in the implementation of AI systems.

Discussion

Legal definitions

The integration of artificial intelligence techniques and technologies with geospatial data and analysis is referred to by the term "GeoAI". The integration of AI and geographic information systems (GIS) is referred to as AI GIS. However, the term "artificial intelligence" is explained variously. International agreements focus on the term "artificial intelligence system" (Szpor, 2023).

In the European Union, there is a legal definition – adopted in June 2024 in the Artificial Intelligence Act (Regulation (EU) 2024/1689) – that states: AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments (Art. 3 (1)). The Polish language version of this definition have been unnecessarily broadened („system AI" oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu…). Despite the drawbacks of translation, the emergence of an EU legal definition makes it possible to increase the consistency of legal regulation and the unambiguity of prospective acts, including the provision of cyber security.

If a geographic information system (GIS) falls within the definition of an AI system from the EU Regulation, then – in addition to previous legislation – its creation and operation is regulated by the AI Act. It also requires the use of 68 terms defined in the EU Regulation in the sense adopted there.

The obliged entities are, in particular, the provider and deployer, whereas the 'provider' means a natural or legal person, public authority, agency, or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of chargé (Art. 3 (3)). The 'deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity (Art. 3 (4)).

Other obligated entities defined in Article 3 are: "authorised representative" (5)," importer" (6), "distributor" (7) and "operator" (8).

Obligations are differentiated according to risk, with the largest concerning "general-purpose AI systems'", "real-time remote biometric identification system' and 'publicly accessible space":

- "general-purpose AI system" means an AI system which is based on a general-purpose AI model, and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems (Art. 3 (66)),
- "real-time remote biometric identification system" means a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention (Art. 3 (42)),
- "publicly accessible space" means any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions (Art.3 (44)), whereas this definition has changed during the legislative process (Szpor, 2023).

It should be noted that – according to the AI Act – systems intended to be used solely to enable cybersecurity and personal data protection measures should not be considered high-risk AI systems. The term 'cybersecurity' occurs 48 times in this act, meaning „the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats". 'Cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons (Regulation (EU) 2019/881, art. 2). The AI Act identifies various cyber threats that necessitate a proactive approach to the cybersecurity of AI systems (Szafrański, 2023).

On the other hand, in official documents issued after the adoption of the AI Act, there are new terms that require explanation, such as: 'Splinternet' – the fragmentation of the open Internet into fragmented networks under the control of governments or corporations) or 'Hyperconnectivity' encompassing both the mediation of ICT in human interaction and the intensification of human-machine and machine-to-machine

interaction (the Internet of Things), which translates into the growing importance of data and the load on telecommunications networks (Strategia cyfryzacji Polski, 2024).

Global regulatory trends and leaders of AI juridization

Artificial intelligence systems have been the subject of intense regulation for the past decade. The first phase was prospective acts: strategies, plans, and programs. The second phase was soft acts on ethical principles (codes, guidelines, recommendations). In the third phase, comprehensive legislation is being developed: conventions, regulations, and laws, into which soft instruments, such as codes of practice, are also incorporated. AI development plans and soft law regarding its ethical aspects even now continue to be relevant (Szpor& Besiekierska 2024; Marchant & Gutierrez, 2023).

The OECD and EU led the way in shaping ethical standards, and other countries (including China) followed suit in creating their acts. The first comprehensive normative acts were adopted by the EU and the Council of Europe. By mid-2024, work was underway on such acts in many countries, including China, Russia, India and the US. Earlier US regulatory restraint was rationalised by initial leadership in AI development and use.

In contrast, AI prospective acts appeared in authoritarian countries: China and Russia earlier than in the EU (Szpor & Besiekierska, 2024). In China in July 2014, the State Council adopted a program to build the "Social Credit System" for 2014-2020, a complex system that tracks human activity holistically using invasive forms of artificial intelligence (social scoring). In May 2015, the State Council adopted a 10-year strategy for modernizing China's manufacturing sector, "Made in China. 2025" (MIC 2025), which targets China to become a world leader in high-tech by 2030. In July 2017, the State Council adopted a detailed "Next Generation Artificial Intelligence Development Plan". Since then, a series of subsequent government acts targeting a specific type or application of AI have been adopted. In 2023. The Ministry of Science and Technology launched a special implementation of "AI for Science" to accelerate innovation and promote high-level application of artificial intelligence in key industries. In 2024, the Ministry of Industry published a draft of 50 national and industry standards for AI, planned for adoption by 2026.

In Russia, extensive plans to obtain the ability to control the digital world were revealed in 2012. According to news published in 2012, Russia's foreign intelligence service then undertook the construction of a system for manipulating mass consciousness through social networks that included: – monitoring the content of the blogosphere and social networks, – studying the processes of community formation and information dissemination in social networks, – determining the factors that influence the popularity and breadth of information dissemination, – working out the methods of organising and directing a virtual 'community of experts' on the Internet, which serve to set tasks and control work in social media, as well as to receive regular information from experts on set topics, – uploading to social networks messages deemed useful by those controlling the cyber-operation to achieve its purpose (Szpor, 2016). Subsequent prospective acts marking the development of AI in Russia include: "Strategy of Scientific and Technological Development of the Russian Federation" dated December 1, 2016 (Decree (ukaz) of the

President of the Russian Federation № 203), 'Strategy of Information Society Development in the Russian Federation for 2017–2030' dated June 6, 2017 (Decree of the President of the Russian Federation), 'Digital Economy of the Russian Federation' – the program dated July 28, 2017 (Decree of the Government of the Russian Federation № 1632 r.), "National Strategy for the Development of Artificial Intelligence until 2030" dated 10.10.2019 (Decree of the President of the Russian Federation № 490), the revision of which, announced in March 2024, is to include, among other things, the creation of its own language model and 10 supercomputers.

In authoritarian states, planning AI systems development as a tool for control in both domestic and foreign policy has been a case for a decade. (Cupać et al., 2024). A comparative analysis of various countries' AI development strategies identified specific motivations for their development. Among others, in the United States, the private sector is strengthened thanks to the lack of restrictive regulations on data processing and close cooperation with the military. In France – maintaining a leading role in science and developing basic research around AI. In Japan – maintaining leadership in robotics, increasing industrialisation, and supporting an ageing population. In the United Arab Emirates, relevant competencies in the Middle East are being built, and a presence in the global value and manufacturing chain is being established (DigitalPoland, 2018; Kabalisa & Altmann, 2021).

In the European Union, the Europe 2020 strategy and one of its programs, the European Digital Agenda, were implemented since 2010, but AI was not exposed in it. It was only in 2018 that the EU "Coordinated Plan on Artificial Intelligence" was adopted, and on its basis, national plans were developed, although in some European countries, France, the UK or Finland, such strategies have already been adopted earlier (DigitalPoland, 2018). The 2021 review noted the great "fragmentation" of national plans. It also already recognized the need to orient EU prospective acts towards increasing resilience. Both AI and cybersecurity were included as specific objectives in later EU prospective acts: Regulation (EU) 2021/694 of the European Parliament and of the Council of April 29, 2021, establishing the "Digital Europe" program and repealing Decision (EU) 2015/2240 and Decision (EU) 2022/2481 of the European Parliament and of the Council of December 14, 2022, establishing the policy program "Road to the Digital Decade" by 2030 (Instruments, 2022).

However, the combination of AI tools with online platforms now enables influencing the election results of public authorities (Jungherr et al., 2024) and threatens the stability of democratic political-organisational systems (Adam & Hockuard, 2023).

Policy for the development of artificial intelligence in Poland

Poland has had an Integrated State Informatisation Programme since 2014, in which the term AI (Artificial Intelligence) did not appear (Martysz et al., 2015). In 2018 Digital Poland Foundation presented a report: 'An overview of strategies for the development of artificial intelligence worldwide'. (DigitalPoland, 2018). It compares the AI development strategies of 9 countries (Canada, China, France, the United States, Japan, the United Kingdom, Finland, South Korea, and the United Arab Emirates). Noting the varying

motivations for developing AI strategies, the key elements each strategy should have were listed, and the following were identified as characteristics of the best 'innovation hubs' for AI development: promotion of a knowledge-based economy, focus on collaboration, cooperation and exchange of experience, availability of data and facilitation of data sharing, pro-business legislation allowing for pilots and experimentation, support for the initiative from the government through to the regional and local levels, respect for intellectual property, public acceptance of the use of modern technology and work automation, a culture of innovation manifested, among other things, in the social acceptance of failure and the acceptance of the use of new technologies. Among other things, social acceptance of failure, provision of comprehensive funding (VCs, accelerators, scale-ups, spin-offs, grants, not only state budgets), close integration of the world of science and research with business and accelerated commercialisation of the results of work, availability of training and a comprehensive approach to science and education, including the availability of a talent forge.

These findings were partially reflected in Resolution No. 196 of the Council of Ministers of December 28, 2020, on the establishment of "Policy for the development of artificial intelligence in Poland from 2020" (Uchwała nr 196, 2020). This Policy describes the activities that Poland should implement and the goals it should achieve in the short term (until 2023), medium term (until 2027) and long term (after 2027), aimed at the development of Polish society, Polish economy and Polish science in the field of artificial intelligence.

All goals and tools are divided into six areas: 1. AI and society 2. AI and innovative companies 3. AI and science 4. AI and education 5. AI and international cooperation 6. AI and the public sector. The document identified 75 goals and 192 tools for achieving them. The draft report for 2020–2023 states that 65 of the 75 goals have been met. However, according to comments on that draft: "the lack of the indicated accountability conditions of the AI Policy leads to limited possibilities for analyzing the contributions of individual government offices. Therefore, the material presented should be regarded as a collection of activities of offices that, according to their interpretation, fall within the scope of the AI Policy's implementation. At this stage, it is not possible to determine whether and to what extent the AI Policy has been implemented."

Among the main goals of the 2020 Resolution of the RM. Policy for the Development of AI in Public Sector Institutions included "efficient and rapid access to data." It sets a strategy for "opening up public data, improving the competence of public administration employees or responsible use of AI solutions by public institutions" (DigitalPoland, 2023). On the other hand, security goals were linked mainly to analytical and information activities.

Public bodies (the President of the Office for Personal Data Protection, Ministry of Finance) and NGOs have drawn attention to the lack of risk analysis in 2024 and the need for greater consideration of the aspect of personal data protection and cybersecurity in further AI development policy (Lewkowicz, 2024; Łukasik & Korgul, 2024).

The conclusions of the implementation of the AI Policy in 2021–2023 emphasized that the following are crucial for the AI Policy: the proper definition of the objectives of

the strategy and the preparation of the mechanisms necessary to ensure agility, manage the strategy and bring about its effective implementation.

In particular, the following need to be refined: accountability, coordination capacity, financing and measurement mechanism: assigning authority to coordinate and implement the policy, human and financial resources, responsibility for task implementation, and developing a measurement mechanism – tools to monitor the progress of AI Policy implementation.

These conclusions should be taken into account by the Working Group on Artificial Intelligence (GRAI) at the Ministry of Digitalization, which has started work on preparing a new AI Policy for Poland in 2024.

The Resolution of the Polish government on the AI Development Policy in Poland was the basis for the government's position in the European Parliament's work on the AI regulation. After the adoption of the AI Act, the competencies of the minister responsible for informatisation (Minister of Digitalization) included the preparation of a national law and both the coordination of AI development policy. A draft law on artificial intelligence systems was presented, creating, among other things, legal safeguards against the use of AI in cyber operations (Projekt ustawy, 2024).

A draft strategy for digitalization has been newly published (Strategia cyfryzacji Polski, 2024). The great merit of this document is its compliance with theoretical findings, including the demands of comprehensiveness. The strategy is not limited to the scope of the government administration department's informatization, taking into account its horizontal impact on society, the state, and the economy. Thus, the name 'strategy of the digital transformation' would be more appropriate. Also because in Polish the term 'cyfryzacja' is equivalent to 'digitisation' (transcription from analogue to digital notation), digitalisation (automatic data processing), and both.

The strategy distinguishes between Diagnosis, Challenges and Trends, SWOT Analysis, Objectives and Enabling Factors, Horizontal Areas (Electronic Communications, Competences of the Future, Cyber Security, Coordination of the Digital Transformation of the Country), 3 Levels: State, People, Business and Technology (under which 17 'other objectives of the Strategy' are grouped), Implementation System, Funding and Glossary.

The term "AI" appears more than 80 times in the strategy. It is one of the areas singled out under 'business and technology' but also appears in other sections.

Cyber-security issues are prominently featured. It is pointed out that the digital sphere is a key field of intensifying geopolitical rivalry, and investments in this area indirectly (through dual-use technologies) or directly translate into the level of state security. It is, therefore, assumed that the key objectives for the next decade must take into account the growing challenges to state security and the priorities of the European Union.

Conclusions

AI systems are subject to multi-level regulation by law. The year 2024 has initiated the phase for adopting comprehensive, universally applicable legislation worldwide. In the EU, the primary act is currently the Regulation – AI Act. It includes nearly seventy definitions, which enhance terminological consistency and clarity of provisions and facilitate the application of the law, including the necessity for cybersecurity

Plans for the development of AI and soft law on its ethical aspects, which dominated the legislation until recently, are now less critical but remain relevant. The structural components of these acts are similar. Based on comparative analysis, conclusions are made about the determinants of their greater or lesser effectiveness. These findings help draft and evaluate new prospective acts. Relating them to the EU and Poland, as its member state, one can see the diagnosis of shortcomings and attempts to reduce them in the next AI development plan. On the other hand, references to AI systems in comprehensive strategies are being intensified; for example, they appear in all parts of the draft comprehensive strategy for Poland's digital transformation.

The motivations for formulating strategies to develop artificial intelligence systems vary across different countries. In authoritarian states, planning involves the development of artificial intelligence systems as tools for guiding policy. In democratic states, plans focus on the economic and social benefits of AI applications. The current economic potential of AI is assessed differently, from enthusiastic predictions to extreme skepticism. However, no one disputes that there are risks associated with its development. The coupling of AI tools with online platforms makes it possible to influence the results of public authorities' elections and threatens the stability and even survival of democratic political-organizational systems. In planning for digital transformation, countering this threat should be a priority. It is necessary to maximize the effectiveness of cybersecurity mechanisms in implementing the AI Act and shaping AI development policies in the European Union and its member states.

References

Adam M., Hockuard C. (2023). European Parliamentary Research Service. Artificial intelligence, democracy and elections. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf (access: 23.12.2024).

Cupać J., Hendrik Schopmans H., Tuncer-Ebetürk İ. (2024). Democratization in the Age of Artificial Intelligence: Introduction to the Special Issue. Democratization, vol. 31, no. 5., pp. 899–921. doi:10.1080/13510347.2024.2338852 (access: 23.12.2024).

DigitalPoland (2018). Przegląd Strategii Rozwoju Sztucznej Inteligencji na Świecie (*Overview of the World Artificial Intelligence Development Strategy*), 2018 https://digitalpoland.org/assets/publications/przegl%C4%85d-strategii-rozwoju-sztucznej-inteligencji-na-swiecie/przeglad-strategii-rozwoju-ai-digitalpoland-report.pdf (access: 15.11.2024).

DigitalPoland (2023). Technologia w służbie społeczeństwu. Czy Polacy zostaną społeczeństwem 5.0? (Technology in the Service of Society. Will Polish People Become Society 5.0?) https://digitalpoland.org/publikacje/pobierz?id=361d97e9-ca5e-4614-afd9-d9d506c66033 (access: 15.11.2024).

Gen AI: too much spend, too little benefit? (2024). Goldman Sachs Global Macro Research. https://www.goldmansachs.com/images/migrated/insights/pages/gs-research/gen-ai--too-much-spend,-too-little-benefit-/TOM_AI%202.0_ForRedaction.pdf (access: 15.11.2024).

Global Views on A.I. (2023). Ipsos Report. https://www.ipsos.com/sites/default/files/ct/news/documents/2023-07/Ipsos%20Global%20AI%202023%20Report.pdf (access: 15.11.2024).

Instruments of Public Law: Digital Transformation during the Pandemic. I. Lipowicz, G. Szpor, A. Syryt (ed.). Routledge, London, 2022. Abingdon, New York, 2023.

Jungherr A., Rauchfleisch A., Wuttke A. (2024). Deceptive uses of Artificial Intelligence in elections strengthen support for AI ban. arXiv preprint arXiv:2408.12613 [access: 23.12.2024).

Kabalisa R., Altmann J. (2021). AI Technologies and Motives for AI Adoption by Countries and Firms: A Systematic Literature Review. In: Tserpes K., et al. Economics of Grids, Clouds, Systems, and Services. GECON 2021. Lecture Notes in Computer Science, vol. 13072. Springer. https://doi.org/10.1007/978-3-030-92916-9_4 (access: 23.12.2024).

Lewkowicz M.B. (2024). Trwają prace nad nową Polityką AI. Co z bezpieczeństwem danych? (*Work on a new AI Policy is underway. What about data security?*). https://cyberdefence24.pl/cyberbezpieczenstwo/trwaja-prace-nad-nowa-polityka-ai-co-z-bezpieczenstwem-danych (access: 15.11.2024).

Łukasik K., Korgul K. (2024). Stosunek Polaków do wykorzystania sztucznej inteligencji w administracji publicznej (*The attitude of Polish people towards the use of artificial intelligence in public administration*). Polski Instytut Ekonomiczny, Warsaw. https://pie.net.pl/wp-content/uploads/2024/09/Sztuczna-inteligencja-w-administracji-publicznej.pdf (access:15.11.2024).

Marchant G.E., Gutierrez C.I. (2023). Soft Law 2.0: An Agile and Effective Governance Approach for Artificial Intelligence. Minnesota Journal of Law, Science and Technology, vol. 24, no. 2., pp. 375–424.

Martysz Cz., Szpor G., Wojsyk K. (2015). Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz (*Act on computerization of activities of entities performing public tasks. Commentary*). Warsaw.

Projekt ustawy o systemach sztucznej inteligencji (*Draft Act on Artificial Intelligence Systems*). https://legislacja.rcl.gov.pl/projekt/12390551/katalog/13087901 (access: 24.10 2024).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151/15 of 7.6.2019.

Regulation (EU) 2021/694 of the European Parliament and of the Council of April 29, 2021 establishing the "Digital Europe" program and repealing Decision (EU) 2015/2240 and Decision (EU) 2022/2481 of the European Parliament and of the Council of December 14, 2022 establishing the policy program "Road to the Digital Decade" by 2030, OJ L 166/1 of 11.5.2021.

Regulation (EU) 2024/1689 of the European Parliament and af the Council 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.

Strategia Cyfryzacji Polski (*State Digitalisation Strategy*) (2024). https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku (access: 15.11.2024).

Szafrański B. (ed.) (2023). Cyberbezpieczeństwo. Redefinicja zagrożeń (*Cybersecurity: Redefining Threats*). Warsaw.

Szpor G. (2023). European legal framework for the use of artificial intelligence in publicly accessible space. GIS Odyssey Journal, vol. 3, no. 2, pp. 25–36. https://doi.org/10.57599/gisoj.2023.3.2.25

Szpor G. (2016). Jawność i jej ograniczenia. Idee i pojęcia. T.1 (*Transparency and its limitations. Ideas and concepts. Vol. 1*). Warsaw.

Szpor G., Besiekierska A. (2024). Prawne instrumenty rozwoju i wykorzystania sztucznej inteligencji a cyberbezpieczeństwo (*Legal instruments for the development and use of artificial intelligence and cybersecurity*). In: AI a cyberbezpieczeństwo (*AI and Cybersecurity*), B. Szafrański (ed.). Warsaw.

Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. w sprawie ustanowienia Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020 (*Resolution No. 196 of the Council of Ministers of 28 December 2020 on the establishment of the Policy for the development of artificial intelligence in Poland from 2020*). M. P. 2021, item 23).