

DOI: 10.31648/kpp.12912

Robert Lizak

Uniwersytet Pomorski w Słupsku

ORCID: 0000-0001-7980-2409

robert.lizak@upsl.edu.pl

Strategic competitiveness between the EU and the United States in artificial intelligence development – human capital, legal frameworks and data

Introduction

The literature emphasizes that artificial intelligence is a so-called general-purpose technology that can influence the transformation of many economic sectors and institutional systems¹. In turn, the literature on technological security indicates that digital technologies, including AI, belong to the category of dual-use technologies that can be used in both the civilian and military sectors². It's impossible not to mention the ongoing race for AI technology dominance, particularly between the United States and the People's Republic of China (PRC). Furthermore, AI has been recognized not only as the most powerful tool in human history for expanding knowledge, increasing prosperity, and enriching the human experience³, but also as a tool that can virtually unlimitedly expand the so-called Window of Vulnerability⁴. Finally, AI is currently

¹ E. Brynjolfsson, A. McAfee, *The business of artificial intelligence. What it can – and cannot – do for your organization*, „Harvard Business Review” 2017, July 18; I. Cockburn, R. Henderson, S. Stern, *The impact of artificial intelligence on innovation*, „National Bureau of Economic Research” 2018, March.

² W.C. McFadden, *Dual-use technologies and national security*, [in:] C.W. Wessner (ed.), *International friction and cooperation in high-technology development and trade: papers and proceedings*, Washington 1997.

³ E. Schmidt (chair), *Final report. National Security Commission on Artificial Intelligence*, March 1, 2021, pp. 10–11.

⁴ S. Manzuik, A. Gold, C. Gatford, *Network security assessment*, pp. 1–16, <https://lira.epac.to/DOCS-TECH/Security/Network%20Security/Network%20Security%20Assessment%20-%20From%20Vulnerability%20to%20Patch.pdf> (accessed: 12.08.2025); R.H. Johnson, *Periods of peril: the window of vulnerability and other myths*, „Foreign Affairs” 1983, Vol. 61, No. 4, pp. 950–970, DOI: 10.2307/20041562.

the technology that most facilitates achieving strategic competitiveness⁵. As can be seen, artificial intelligence, as the most transformative general-purpose technology and at the same time a dual-use weapon, has now become a key, even decisive factor in achieving and maintaining the strategic competitiveness of states.

According to D. Faulkner and C. Bowman, strategic competitiveness is the ability of an organization to outperform its competitors. While the global battle for supremacy in the AI field has been fought in recent decades between China and the United States⁶, in September 2024, the European Union (EU) also attempted to join this fight by publishing the „European Competitiveness Strategy”, hereinafter referred to as the „Draghi Report”⁷. Although the strategy covered practically all sectors of the EU economy with recommendations for improving their functioning, three sectors were considered key⁸, including bridging the growing investment gap between the EU and the United States and China, especially in the area of AI. For example, AI is currently used by only 11% of businesses in the EU, while 73% of the core AI models developed since 2017 come from the United States and 15% from China⁹.

This article attempts to assess the state of strategic competitiveness of the EU and the United States in the field of AI, based on a review of EU law and data contained in the Draghi Report, and compares them with US federal law and available data contained in federal government documents. The legal issue analyzed in this article is whether the regulatory frameworks for artificial intelligence adopted in the European Union and the United States differentially impact the ability of these legal systems to support the development of AI technologies. In other words, the analysis addresses the question of whether differences in regulatory design – particularly regarding access to human capital, data protection, and data availability – may impact the level

⁵D. Faulkner, C. Bowman, *Strategie konkurencji*, Warsaw 1996, pp. 35–37.

⁶Cf. E. Schmidt, op. cit.; H. Kissinger, E. Schmidt, D. Huttenlocher, *The age of AI: and our human future*, London 2022.

⁷M. Draghi, *The future of European competitiveness. Part A. A competitiveness strategy for Europe*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en (accessed: 12.08.2025); idem, *The future of European competitiveness. Part B. In-depth analysis and recommendations*, https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en (accessed: 12.08.2025).

⁸The other two sectors concern the decarbonisation of the economy, which will increase the competitiveness of the EU, as well as strengthening security, understood both in the military sense. Cf. M. Draghi, *The future of European competitiveness. Part A...*, pp. 6–7.

⁹The Draghi report pointed out that there is a risk that Europe will become entirely dependent on AI models designed and developed abroad, both for general-purpose AI and, gradually, for vertical applications dedicated to key EU sectors, including automotive, banking, telecommunications, healthcare, mobility, and retail. For example, AI is currently used by only 11% of EU companies, while 73% of the core AI models developed since 2017 come from the United States and 15% from China. Another example is the volume of capital invested in AI in 2016, when AI investment in Europe reached €3–4 billion (€6.5–9.7 billion in Asia) and €15–23 billion in the United States, while the volume of venture capital invested in 2023 was \$8 billion in the EU (\$15 billion in China) and \$68 billion in the United States. See: LEAM:AI, *Large AI models for Germany – feasibility study 2023*, 2023; *Artificial Intelligence Index Report 2024*, Stanford University, 2024; M. Draghi, *The future of European competitiveness. Part B...*, p. 79; *Digitization, AI, and the future of work: imperatives for Europe*, briefing note, McKinsey Global Institute, September 2017, p. 4.

of technological competitiveness of both economies. The article adopts the assumption that legal regulation constitutes not merely a framework for governing AI, but one of the determinants of strategic competitiveness. Accordingly, the comparative analysis focuses not only on identifying regulatory differences but also on assessing how those differences may influence innovation capacity, commercialization of AI technologies and long-term economic competitiveness.

The literature indicates that the development of artificial intelligence is determined primarily by three groups of factors: the availability of highly qualified human capital, a regulatory environment conducive to innovation, and access to large data sets necessary to train AI models¹⁰. For the purposes of this article, a review of selected US and EU legal acts relevant to the development of artificial intelligence was conducted. The comparative legal analysis is complemented by a functional assessment of the potential impact of selected regulations on innovation capacity and strategic competitiveness. Due to the dynamic nature of AI regulations, the analysis extensively utilized strategic documents, public institution reports, and statistical data, which constitute the primary sources of knowledge about public policies in the area of technology. This allowed us to determine the scope of the legal and political approach to AI in the US and the EU. In the author's opinion, the added value of this publication is the presentation of proposed recommendations for the EU. A strategic approach to accumulating human capital for AI development

The Draghi Report argues that the EU has a low total number of new researchers in the field of Data Science compared to the United States, in particular, the talent pool needed to develop AI in the EU is smaller, as highly qualified specialists are often „captured” to the United States, for example by offering high salaries¹¹. US federal law has introduced a number of laws aimed at accumulating human capital, including, for example, through AI-related education and workforce development¹². The National Artificial Intelligence Initiative Act of 2020 established a federal system for coordinating AI research and collaborating between government, universities, and the private sector. Among other things, the act provides for the creation of a national AI research initiative, the development of educational programs, and increased funding for AI research¹³.

¹⁰ Cf. W. Nowakowski, *Wykorzystanie sztucznej inteligencji przez małe i średnie firmy w Europie*, [in:] T. Doligalski, D. Kaszyński (eds.), *Sztuczna inteligencja w przedsiębiorstwach i gospodarce (AI SPRING 2024)*, Warsaw 2025, pp. 73–91; P. Hacker, *A legal framework for AI training data – from first principles to the Artificial Intelligence Act*, „Law, Innovation and Technology” 2021, Vol. 13, Issue 2, pp. 257–301.

¹¹ M. Draghi, *The future of European competitiveness. Part B...*, p. 79.

¹² See: § 7(b) Executive Order 13859 of 2019, Maintaining American Leadership in Artificial Intelligence.

¹³ See: § 2(9) National Artificial Intelligence Initiative Act of 2020. Cf. R. Lizak, *Prawne aspekty neuronowego modelu zarządzania danymi w administracji federalnej Stanów Zjednoczonych z wykorzystaniem AI*, Warsaw 2024, pp. 217–257.

The publication of the Draghi Report was followed by the AI Continent Action Plan adopted by the European Commission in April 2025¹⁴. The Action Plan demonstrates that the EU has recognised that legal regulation alone is insufficient to strengthen strategic competitiveness. Consequently, it complements the AI Act with measures aimed at expanding computing infrastructure, improving access to high-quality data, attracting talent and supporting AI commercialisation. This evolution suggests a gradual shift from a predominantly regulatory approach towards a more innovation-oriented policy.

On 13 June 2024, Regulation (EU) No. 2024/1689 of the European Parliament and of the Council, known as the „EU AI Act”, was adopted, constituting the first legal act regulating the issue of AI, which obliges EU Member States to provide providers, entities and persons using AI with the necessary competences to enable them to make informed decisions in relation to AI systems¹⁵. A key element of the EU AI Act is the risk classification system for AI systems. According to Article 6 of the regulation, AI systems can be classified as high-risk if their use could have a significant impact on fundamental rights or public security. In such cases, AI system providers are required, among other things, to implement a risk management system (Article 9) and ensure the appropriate quality of data used to train algorithms (Article 10)¹⁶.

Additionally, the EU AI Act includes a definition of AI competences, which defines them as the skills, knowledge, and understanding that enable providers, users, and individuals affected by AI – taking into account their rights and obligations under this regulation – to thoughtfully deploy AI systems and be aware of the opportunities, risks, and potential harm AI can cause. Furthermore, the EU clarifies that implementing AI systems in education is important to promote high-quality digital education and training and to enable all learners and teachers to acquire the necessary digital skills and competences, including media literacy, critical thinking, and the ability to share these skills and competences, for active participation in the economy, society, and democratic processes. The EU has also undertaken a number of research and innovation initiatives related to human capital, as exemplified by Horizon Europe, the Digital Europe Programme, and Erasmus+.

The comparison demonstrates that both legal systems recognize human capital as a strategic resource; however, they pursue different regulatory priorities. While the US legal framework primarily seeks to attract and retain top AI talent through market-oriented mechanisms, the EU focuses on broad competence development and responsible

¹⁴AI Continent Action Plan, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee Of The Regions, Brussels, 9.4.2025, COM(2025) 165 final.

¹⁵Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) (WE) No. 300/2008, (UE) No. 167/2013, (UE) No. 168/2013, (UE) 2018/858, (UE) 2018/1139 and (UE) 2019/2144 and directives 2014/90/UE, (UE) 2016/797 and (UE) 2020/1828 (Dz.U. UE L 2024/1689, 12.7.2024).

¹⁶Cf. S. Wachter, B. Mittelstadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, „International Data Privacy Law”2017, Vol. 7, Issue 2, pp. 76–99.

deployment of AI. These differences directly affect the ability of both jurisdictions to compete for highly qualified specialists. It should be noted that the publication of the Draghi Report has already begun to influence subsequent EU regulatory policy. In April 2025, the European Commission adopted the AI Continent Action Plan, which complements the AI Act with measures aimed at strengthening Europe's technological competitiveness through investments in AI infrastructure, high-quality datasets, AI Factories, Gigafactories and talent development. Moreover, the ongoing simplification of the AI Act implementation under the Digital Omnibus initiative demonstrates that the EU itself has recognised the need to reduce regulatory burdens while maintaining a high level of protection of fundamental rights. These developments appear to confirm the central argument advanced in this article that strategic competitiveness requires not only effective regulation, but also a legal and institutional framework capable of supporting innovation and commercialization¹⁷.

A strategic approach to creating laws that support AI development

US federal law has adopted a number of laws to facilitate the development of AI by creating a dedicated legal environment for this technology. One example is the DATA Act¹⁸. The purpose of this initiative is to: 1) make public all direct and indirect expenditures resulting from federal grant and loan agreements; 2) establish a national standard for financial data to be presented in a reliable, credible, and searchable manner; 3) simplify reporting; 4) establish sanctions for unreliable data provided on USAspending.gov¹⁹.

Another act is the OPEN Government Data Act, the purpose of which is to make the federal government's database resources publicly available, which are published in machine-readable form, excluding data from certain government institutions, especially intelligence and military ones²⁰. Finally, it is necessary to mention the Evidence Act, which was passed to improve the process of data collection within the framework of the federal government's activities by improving access to data and increasing the possibilities of their processing²¹. In other words, the purpose of the Evidence Act is to change the model of management of collected data by the federal government by strengthening the coordination of data exchange between federal agencies in order

¹⁷ Artificial Intelligence, Council and Parliament agree to simplify and streamline rules, Council of the EU, Press release, 7 May 2026.

¹⁸ Digital Accountability and Transparency Act of 2014, Public Law 113-101, 113th Congress, [S. 994], May 9, 2014.

¹⁹ USAspending.gov is a government website that provides current data on federal government spending and allows you to verify the purpose of public spending and its beneficial owners, usaspending.gov (accessed: 12.08.2025).

²⁰ Open, Public, Electronic, and Necessary Government Data Act, Public Law 114-396, 114th Congress, 2d Session, [S. 2852], December 11, 2016.

²¹ Foundations for Evidence-Based Policymaking Act, the 115th U.S. Congress, Public Law 2019, No. 115, p. 435.

to enable the process of transforming data into information, and information into knowledge, which facilitates decision-making, including in the strategic dimension.

In addition, six federal laws were adopted in the United States federal law between 2018 and 2023²² and three executive orders of the President of the United States with the force of law²³, which directly concern AI, with the most attention paid to the economy, science, work and civil liberties²⁴. Finally, in 2025, EO 14192 was adopted, which requires that for each new regulation issued, at least 10 existing regulations be identified to be repealed²⁵. It added that in fiscal year 2025, the leadership of all federal agencies is required to ensure that the total incremental cost of all new regulations to be enacted this year, as well as repealed regulations, is significantly less than zero, unless otherwise specified by law or instructions from the Director of the Office of Management and Budget. It is impossible to avoid the impression that this approach to deregulation in the United States directly impacts the development of AI²⁶. The Draghi report rightly points out that deregulation is extremely important for the development of AI, because greater „regulatory flow” – defined as the number of new regulations passed in a given period – is one of the factors that significantly reduces the dynamics of AI development²⁷.

As can be seen, the EU significantly outpaces the United States in the number of new legal acts adopted, although it should be borne in mind that before drawing more detailed conclusions, the volume of these acts and their scope should be examined. The Draghi Report paid particular attention to the General Data Protection Regulation (GDPR), and subsequently identified the three greatest regulatory challenges faced by EU businesses, including:

- compliance with a growing number of EU laws and their frequent changes over time, resulting in overlapping regulations and legal inconsistency,

²² See: Identifying Outputs of Generative Adversarial Networks Act (IOGAN Act), 116th Congress, Public Law 116-258, S. 2904, December 23, 2020; National Artificial Intelligence Initiative Act of 2020, H.R.6216, 116th Congress, December 3, 2020; AI in Government Act of 2020, H.R.2575, 116th Congress, September 14, 2020; National AI Research Resource Task Force Act of 2020, 116th Congress, Public Law 116-283, S. 3890, January 1, 2021; Artificial Intelligence Training for the Acquisition Workforce Act, 117th Congress Public Law, Public Law 117-207, S. 2551, October 17, 2022; Advancing American AI Act, 117th Congress, Public Law 117-270, S. 1353, December 19, 2022.

²³ See: Executive Order 13859 of February 11, 2019, Maintaining American Leadership in Artificial Intelligence; Executive Order 13960 of December 3, 2020, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government; Executive Order 14110 of October 30, 2023, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

²⁴ See: R. Lizak, *Prawne aspekty...*, pp. 113–119.

²⁵ Executive Order 14192 of January 31, 2025, Unleashing Prosperity Through Deregulation.

²⁶ R. Lizak, *Redukcja inflacji prawa z wykorzystaniem AI w Stanach Zjednoczonych na tle raportu Dragiego dla Unii Europejskiej*, „Kortowski Przegląd Prawniczy” 2025, No. 4, pp. 141–156.

²⁷ During the last three terms of the United States Congress, from 2019 to 2024, approximately 3,500 pieces of legislation and approximately 2,000 resolutions were passed at the federal level. Meanwhile, during the same period, the EU adopted approximately 13,000 pieces of legislation, of which 515 were ordinary legislative acts, 2,431 were other legislative acts, 954 were delegated acts, 5,713 were implementing acts, and 3,442 were other legal acts. See: M. Draghi, *The future of European competitiveness. Part B...*, p. 318; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Identifying and addressing barriers to the Single Market, SWD(2020) 54 final, COM(2020) 93 final, European Commission, Brussels, 10.3.2020.

- additional burdens resulting from national transposition and enforcement, including „over-implementation” of EU laws by Member States, as well as divergent implementation requirements and standards across Member States²⁸,
- proportionally higher regulatory burdens that medium and small enterprises have to cope with compared to larger enterprises²⁹.

In the case of the GDPR, it has also been noted that there is a lack of consistency in the enforcement of the regulation by Member States, which increases the administrative burden on businesses in the EU. While the GDPR aims to provide a harmonized EU approach to privacy enforcement, the regulation allows Member States to define privacy rules in 15 areas, leading to fragmentation and legal uncertainty resulting from the widespread use of specification clauses and, consequently, inconsistent enforcement by national data protection authorities³⁰. This hinders cross-border innovation, and the costs of GDPR compliance for EU companies have reduced data storage by 26% and data processing by 15% compared to comparable US companies³¹.

I. Kusche correctly noted that the EU AI Act requires a number of specific measures that will, in practice, hinder or even prevent the development of AI in the EU. The author added that the EU AI Act increases the need for legal analyses and administrative decisions, but these decisions cannot be based on anything more than they would have been without the EU AI Act. Namely, on the one hand, a coherent legal argument balancing fundamental rights, and on the other, the temporary prioritization of certain values over others. I. Kusche also noted that the EU AI Act imposes new obligations on companies when creating and implementing AI systems, although their impact on actual risk remains unclear. Introducing the concept of systemic risk at a late stage of the legislative process for the EU AI Act highlights the ambition for a comprehensive risk mapping, but specifying the meaning of this comprehensiveness in law may prove difficult or even impossible. This is because a particular challenge in ensuring comprehensive risk mapping is the need to bridge the gap between abstract thinking about risk and the concrete formulation of principles that apply to specific AI systems. Finally, the author argues that the AI EU Act opens the door to decisions that, while not necessarily arbitrary, have nothing to do with risk assessment, but are rather negotiations between interest groups that differ significantly in terms of power³².

A summary of the most important legal acts regulating the development of artificial intelligence in the United States and the European Union is presented in the table below.

²⁸ M. Draghi, *The future of European competitiveness. Part B...*, p. 319.

²⁹ Ibidem.

³⁰ Ibidem.

³¹ Importantly, in December 2023, EU Member States, within the Justice and Home Affairs Council, opposed further harmonisation of the GDPR. See: M. Draghi, *The future of European competitiveness. Part B...*, p. 319; Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, European Commission, Brussels, 25.7.2024.

³² See: I. Kusche, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, „Journal of Risk Research” 2024, DOI: 10.1080/13669877.2024.2350720.

Table 1. Selected legal acts regulating the development of artificial intelligence in the United States and the European Union

Regulatory Area	European Union	United States	Regulatory Importance
Regulation of AI systems	EU AI Act (2024/1689)	Executive Order 14179 (2025) ³³	– establishing security and risk management principles for AI systems (EU) – supporting human development, economic competitiveness, and national security (US)
Data protection	RODO (2016/679)	Artificial Intelligence Risk Management Framework (AI RMF 1.0) ³⁴	defining the principles of data processing used by AI systems
Availability of public data	Data Governance Act (2022/868)	OPEN Government Data Act (2019)	increasing the availability of public data for AI development
Technological infrastructure	Digital Europe Programme	CHIPS and Science Act (2022)	supporting the development of computing infrastructure and AI research
AI development policy	EU digital strategy	National AI Initiative Act (2020)	coordination of scientific research and development of AI technologies

Source: own study based on EU and US law.

The presented summary shows that regulations adopted in the European Union are more comprehensive and focused on managing the risks of AI technologies, while American regulations focus primarily on supporting technological innovation and the development of data infrastructure. The comparison presented in Table 1 confirms that the regulatory divergence observed in individual legal acts reflects broader differences in strategic regulatory philosophy. The Draghi report includes criticism from EU businesses regarding the lack of a solution to the main threat to AI development in the EU: the dynamic expansion and consolidation of the enormous power wielded by a few dominant technology companies worldwide, particularly American ones. This is

³³Executive Order 14179 of January 23, 2025, Removing Barriers to American Leadership in Artificial Intelligence.

³⁴Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology, January 2023.

a serious matter because these companies influence individuals' personal lives, the economies of individual countries, and political and legal systems³⁵. Moreover, the Draghi report pointed out that the adoption of the EU AI Act means a lot of additional work and costs for start-ups and small and medium-sized enterprises³⁶. On the one hand, the EU AI Act addresses serious challenges such as AI transparency and ethics. On the other, it imposes overly burdensome obligations on all businesses, despite the introduction of supposed simplifications such as regulatory sandboxes. This raises concerns about the creation of additional regulatory barriers that will be counterproductive, even benefiting American and Chinese competitors. Above all, it will limit the opportunities for European innovators and leaders in AI to emerge³⁷.

These observations indicate that the fundamental difference between both regulatory models lies not in the existence of regulation itself, but in the regulatory philosophy adopted. The EU predominantly uses regulation as a mechanism for mitigating societal risks, whereas the United States primarily treats regulation as an instrument supporting technological development and economic competitiveness. This distinction constitutes one of the principal factors explaining the different innovation dynamics discussed in the concluding section.

A strategic approach to data availability for AI development

In the literature on the digital economy, data is often referred to as a key resource of the digital economy and a fundamental factor in the development of artificial intelligence systems³⁸. The United States federal government processes vast amounts of data that are crucial for assessing the state of the national economy, including data from annual tax returns, censuses, or data necessary to assess the unemployment rate³⁹. Federal government data is not only the main driver of the American economy, as decisions are made based on it, especially political and business ones, but also a driver of AI, because data for AI is like fuel for a combustion engine⁴⁰. In April 2018, the Federal Data Strategy

³⁵ Cf. S. Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, London 2019.

³⁶ This is important because, considering the best global AI startups in the world, 61% of global funding goes to American companies, 17% to Chinese companies and only 6% to those from the EU. See: M. Draghi, *The future of European competitiveness. Part A...*, p. 79 and annotation XXXI.

³⁷ P. Davies, *EU AI Act reaction: tech experts say the world's first AI law is 'historic' but 'bittersweet'*, <https://www.euronews.com/next/2024/03/16/eu-ai-act-reaction-tech-experts-say-the-worlds-first-ai-law-is-historic-but-bittersweet> (accessed: 12.08.2025).

³⁸ Cf. V. Mayer-Schönberger, K. Cukier, *Big data: a revolution that will transform how we live, work, and think*, Boston 2013.

³⁹ The Promise of Evidence-Based Policymaking. Report of the Commission on Evidence-Based Policymaking Appendices E-H, September 2017; Federal Data Strategy 2020 Action Plan, President's Management Agenda, 2020. According to J. Lane and N. Potok, there is an urgent need to create valuable data for the future of American society. See: J. Lane, N. Potok, *Democratizing data: our vision*, <https://hdrs.mitpress.mit.edu/pub/m1o4oblm/release/1> (accessed: 12.08.2025).

⁴⁰ USAFacts is a non-profit organization and website that provides data and reports on the U.S. population, government finances, and government's impact on society, <https://usafacts.org/articles/how-to-use-government-data/> (accessed: 12.08.2025).

was adopted⁴¹. The aim is to establish a framework of operational principles and best practices to support federal agencies in building a coherent data infrastructure and managing it effectively over the next ten years⁴². In the United States, the OPEN Government Data Act of 2019 also plays a significant role in public data management, establishing the principle of publishing public data in a format that allows for automated processing. This regulation is particularly important for the development of artificial intelligence systems, as it allows for the use of large public data sets to train algorithms. At the same time, the Modernizing Government Technology Act (MGT Act) was passed⁴³, the aim of which is to provide financial resources for the modernization of federal IT systems, which would involve increasing efficiency, reducing costs and increasing computing power through cloud computing infrastructure⁴⁴. Obviously, this infrastructure is ultimately intended to facilitate data processing using AI. In the author's opinion, the United States is implementing a neural model of data management in the federal government using AI, which introduces fundamental changes to the way data is managed. Instead of the current silo-based, departmental data management, AI enables distributed processing and sharing of public data, which improves data integration, shortens data transfer times, and reduces the number of administrative processes. This model is based on the artificial neural network model, in which administrative units act as neurons, processing data and making decisions based on AI algorithms⁴⁵.

In the area of data accessibility, the Draghi Report concluded that despite the ambitious objectives of the EU GDPR and the EU AI Act, which are commendable from a social perspective, the stringent data protection provisions of these legal acts, combined with their complexity and inconsistency, may hinder EU action in this area, not least due to the aforementioned inconsistency in GDPR implementation and enforcement. As the „winner takes most” approach to strategic competitiveness in AI dominates, the EU now faces the inevitable question of how to balance the need for data protection and privacy with the need for dynamic growth in innovation in the EU economy. In response, the EU adopted Regulation (EU) 2024/903, which aims to facilitate interaction between EU institutions and bodies and public sector bodies of EU Member States by sharing data, information, and knowledge through digital processes (cross-border interoperability), fostering closer cooperation, and facilitating the smooth flow of data across borders.

⁴¹ President's Management Agenda, Modernizing Government for the 21st Century, 2018.

⁴² The rapid growth in the scale and scope of data-related activities is evidenced by the list of 332,869 public datasets on the data.gov website. The mission of data.gov, or U.S. Government Open Data, is to unleash the power of open government data to inform public and decision-makers about policy decisions, drive innovation and economic activity, advance the missions of federal agencies, and strengthen government openness and transparency. The Home of the U.S. Government's Open Data, <https://data.gov> (accessed: 12.08.2025).

⁴³ Modernizing Government Technology Act of 2017 or the MGT Act, 115th Congress, 2017–2018, H.R.2227.

⁴⁴ Implementation of the Modernizing Government Technology Act, Memorandum for the Heads of Executive Departments and Agencies M-18-12, Executive Office of the President Office of Management and Budget, Washington, February 27, 2018, <https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf> (accessed: 12.08.2025).

⁴⁵ R. Lizak, *Prawne aspekty...*, pp. 113–119.

In the opinion of the author of this publication, due to the dynamic technological progress, especially in the field of AI, it is justified to regularly identify potential regulatory obstacles, particularly in the area of data access, arising from both EU and national legislation. The situation is similar when it comes to the regular and efficient updating of legal provisions concerning AI. Furthermore, consideration should be given to developing simplified obligations for small and medium-sized enterprises. Finally, efforts should be made to ensure a uniform market passporting system for all cloud services provided in the EU and to eliminate the possibility of Member States imposing excessively extensive protection requirements that go beyond the requirements of the GDPR and the EU AI Act.

Conclusion

One of the topics of the current debate on the regulation of artificial intelligence focuses on finding a balance between supporting technological innovation and protecting fundamental rights⁴⁶. The analysis of three areas – human capital, the regulatory environment, and data availability – allows us to draw several conclusions regarding the differences in the approach of the United States and the European Union to the development of artificial intelligence. The analysis of selected legal regulations in the United States and the European Union indicates that the two legal systems have adopted different approaches to regulating AI. In the United States, regulations focus primarily on supporting technological innovation and cooperation between the public and private sectors, while in the European Union, a greater emphasis is placed on protecting fundamental rights and managing the risks associated with the use of AI systems. The more restrictive approach to protecting fundamental rights in the EU also applies to other areas, not just those related to AI⁴⁷.

A review of federal law shows that the United States has established a favorable legal environment for AI development, including in the areas of human capital accumulation, legal favorability, and data availability. This accumulation of human capital influences AI development and increases the dynamics of the American labor market. Collaboration between the private sector and the scientific sector plays a significant role, facilitating the efficient adaptation of training programs to market needs. Finally, the United States is a global leader in recruiting highly skilled workers through visa programs (e.g., H-1B), which strengthens American research and development potential. US federal law directly related to AI is characterized by considerable flexibility, which favors AI development in the private sector.

⁴⁶L. Floridi, J. Cowsls, M. Beltrametti, et al., *AI4People – an ethical framework for a good ai society: opportunities, risks, principles, and recommendations*, „Minds and Machines” 2018, Vol. 28, pp. 689–707, DOI: 10.1007/s11023-018-9482-5.

⁴⁷A. Bradford, *The Brussels effect*, „Northwestern University Law Review” 2015, No. 1, pp. 22–26; M.F. Kightlinger, *Twilight of the idols? EU internet privacy and the post enlightenment paradigm*, „Columbia Journal of European Law” 2007, Vol. 14, No. 114, pp. 2–3.

There is no doubt that the United States is a leader in standardizing AI-related legal norms, and American technology companies, thanks to their dominant position in the global market, exert significant influence on international AI standards and norms, strengthening their global competitive advantage. However, this does not mean that the American model should be considered normatively superior. This article merely argues that under current normative conditions, the American model favors the faster commercialization of AI technologies, which, in turn, may enhance the strategic competitiveness of the United States. In the United States, data is perceived as a strategic resource, which essentially determines the critical need for its unrestricted collection. Although there are numerous legal norms in the United States aimed at protecting data, they are not overly burdensome and provide flexibility in its access and commercial use, especially by technology startups relying on dynamic prototyping and testing of data-driven products⁴⁸.

The EU has undertaken a number of measures aimed at the widespread digitalization of society and aims to create a qualified workforce capable of developing AI. The EU appears to be placing greater emphasis on educating broad social groups, striving to bridge the digital divide and ensure equal access to AI-related education, whereas in the United States, this emphasis has focused on experts and leaders. EU law classifies AI applications according to risk levels and imposes different regulatory obligations depending on the type and characteristics of the technology. Furthermore, the EU promotes the concept of trustworthy AI, which, in line with European values, is expected to operate transparently, responsibly, and in compliance with human rights. Although this approach is socially desirable, the rate of return for companies is significantly lower and longer than in the American model, which may significantly impede compliance with the provisions of EU law and, consequently, limit their competitiveness in the global market.

The preceding analysis confirms the initial research assumption that differences in legal design influence not only the governance of AI systems but also the ability of economies to generate innovation and maintain technological leadership. The strategic competitiveness assessment of AI development in the areas of human capital, law, and data shows that the United States has adopted a more flexible approach to data and private sector support, striving to become a leader in innovation and the commercialization of AI solutions. In the EU, significant attention has been focused on setting ethical standards, which can attract investors interested in sustainable development and technologies compliant with high standards of data protection and human rights. GDPR, which has become a privacy standard and enables an adequate level of data security, is of particular concern. However, it significantly limits companies' access to large data sets, consequently slowing down AI development. While the EU strives to

⁴⁸ Cf. Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. § 552a); Children's Online Privacy Protection Act of 1998, Public Law 105-277, October 21, 1998 (15 U.S.C. §§ 6501-6506); Fair Credit Reporting Act, Public Law 91-508, October 26, 1970 (15 U.S.C. § 1681).

create data-sharing ecosystems between member states that respect ethical and privacy principles, it also places restrictions on access to commercial data. This leads to European companies often struggling to acquire large data sets, limiting their ability to train advanced AI algorithms – the opposite of the situation in the United States.

In summary, it can be assumed that a global race to „tame” AI is currently underway between the United States and the EU. While the EU has the potential to compete with the United States, especially if it revises its ethics and data protection priorities to increase the pace of innovation and recruit talent and leaders, the current level of human capital accumulation in the United States, the degree of legal favorability, and the scope of data access effectively determine the United States’ dominant position relative to the EU. Furthermore, the Draghi report aptly points out that the EU’s weak position in AI development means that in the future, it may not fully leverage its competitive advantage in several industry sectors, which carries the risk of potential market erosion and value-share erosion of EU companies to non-EU entities⁴⁹. Both models have the potential to collaborate on basic research, create common technical standards, and promote responsible use of AI globally. *Prima facie*, such collaboration seems likely to yield benefits both in terms of technological innovation and in building public trust in modern technologies.

Finally, it is worth presenting recommendations for the EU, for each of the areas examined. First, in the area of human capital, the EU should strive to establish a network of AI centers of excellence. These centers should collaborate with universities and the private sector to effectively attract and develop talent, making it more difficult for the United States to recruit them, while simultaneously promoting the interdisciplinary nature of scientific research. The EU should also strive to facilitate talent migration, especially for highly qualified specialists from outside the EU, allowing for more effective competition with other global players for international AI talent. Second, it is recommended to avoid increasing inflation of AI law, striving to maintain a balance between facilitating the dynamic development of AI and maintaining adequate data protection and privacy. Third, in the area of data, the EU should strive to build shared database resources, including those accessible to innovators and researchers. A good example is the Common European Data Spaces initiative, which provides a basis for ensuring common, high-quality data resources⁵⁰. Finally, the EU should actively seek to establish partnerships that will enable the exchange of experiences and knowledge in the use of data and AI. Access to high-quality datasets should therefore be viewed as a strategic legal determinant of AI competitiveness. Consequently, differences in data governance models have implications extending beyond privacy protection, directly influencing innovation capacity and the speed of AI deployment.

⁴⁹M. Draghi, *The future of European competitiveness. Part B...*, p. 79.

⁵⁰Common European Data Spaces, <https://digital-strategy.ec.europa.eu/en/policies/data-spaces> (accessed: 12.08.2025).

REFERENCES

Legal acts

- Advancing American AI Act, Public Law 117-270, 117th Congress, December 19, 2022.
- AI in Government Act of 2020, H.R. 2575, 116th Congress, September 14, 2020.
- Artificial Intelligence Training for the Acquisition Workforce Act, Public Law 117-207, October 17, 2022.
- Children's Online Privacy Protection Act of 1998, Public Law 105-277, October 21, 1998.
- Digital Accountability and Transparency Act of 2014, Public Law 113-101, May 9, 2014.
- Executive Order 8807 Establishing the Office of Scientific Research and Development, June 28, 1941.
- Executive Order 13859 Maintaining American Leadership in Artificial Intelligence, February 11, 2019.
- Executive Order 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, December 3, 2020.
- Executive Order 14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023.
- Executive Order 14179 Removing Barriers to American Leadership in Artificial Intelligence, January 23, 2025.
- Executive Order 14192 Unleashing Prosperity Through Deregulation, January 31, 2025.
- Fair Credit Reporting Act, Public Law 91-508, October 26, 1970.
- Foundations for Evidence-Based Policymaking Act, Public Law 115-435, January 14, 2019.
- Identifying Outputs of Generative Adversarial Networks Act (IOGAN Act), Public Law 116-258, December 23, 2020.
- Modernizing Government Technology Act of 2017, H.R. 2227, 115th Congress.
- National AI Research Resource Task Force Act of 2020, Public Law 116-283, January 1, 2021.
- National Artificial Intelligence Initiative Act of 2020, H.R. 6216, 116th Congress, December 3, 2020.
- Open, Public, Electronic, and Necessary Government Data Act, Public Law 114-396, December 11, 2016.
- Privacy Act of 1974, Public Law 93-579, December 31, 1974.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) (WE) No. 300/2008, (UE) No. 167/2013, (UE) No. 168/2013, (UE) 2018/858, (UE) 2018/1139 and (UE) 2019/2144 and directives 2014/90/UE, (UE) 2016/797 and (UE) 2020/1828 (Dz.U. UE L 2024/1689, 12.7.2024).

Reports and documents

- AI Continent Action Plan, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee Of The Regions, Brussels, 9.4.2025, COM(2025) 165 final.
- Artificial Intelligence: Council and Parliament agree to simplify and streamline rules, Council of the EU, Press release, 7 May 2026.
- Artificial Intelligence Index Report 2024, Stanford University 2024.
- Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology, January 2023.
- Common European Data Spaces, <https://digital-strategy.ec.europa.eu/en/policies/data-spaces>.
- Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, European Commission, Brussels, 25.7.2024.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Identifying and addressing barriers to the Single Market, SWD(2020) 54 final, COM(2020) 93 final, European Commission, Brussels, 10.3.2020.
- Digitization, AI, and the Future of Work: Imperatives for Europe, McKinsey Global Institute, September 2017.
- Federal Data Strategy 2020 Action Plan, President's Management Agenda, 2020.
- Implementation of the Modernizing Government Technology Act, Memorandum M-18-12, Executive Office of the President OMB, Washington, February 27, 2018.
- LEAM:AI: Large AI Models for Germany – Feasibility Study 2023, 2023.
- President's Management Agenda: Modernizing Government for the 21st Century, 2018.
- The Home of the U.S. Government's Open Data, <https://data.gov>.
- The Promise of Evidence-Based Policymaking. Report of the Commission on Evidence-Based Policymaking, September 2017.

Literature

- Bradford A., *The Brussels effect*, „Northwestern University Law Review” 2015, No. 1.
- Brynjolfsson E., McAfee A., *The business of artificial intelligence. What it can – and cannot – do for your organization*, „Harvard Business Review” 2017, July 18.
- Cockburn I., Henderson R., Stern S., *The impact of artificial intelligence on innovation*, „National Bureau of Economic Research” 2018, March.
- Davies P., *EU AI Act reaction: tech experts say the world's first AI law is 'historic' but 'bittersweet'*, <https://www.euronews.com/next/2024/03/16/eu-ai-act-reaction-tech-experts-say-the-worlds-first-ai-law-is-historic-but-bittersweet>.
- Draghi M., *The future of European competitiveness. Part A. A competitiveness strategy for Europe*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en.

- Draghi M., *The future of European competitiveness. Part B. In-depth analysis and recommendations*, https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en.
- Faulkner D., Bowman C., *Strategie konkurencji*, Warsaw 1996.
- Floridi L., Cowls J., Beltrametti M., et al., *AI4People – an ethical framework for a good ai society: opportunities, risks, principles, and recommendations*, „Minds and Machines” 2018, Vol. 28, DOI: 10.1007/s11023-018-9482-5.
- Hacker P., *A legal framework for AI training data – from first principles to the Artificial Intelligence Act*, „Law, Innovation and Technology” 2021, Vol. 13, Issue 2.
- Johnson R.H., *Periods of peril: the window of vulnerability and other myths*, „Foreign Affairs” 1983, Vol. 61, No. 4, DOI: 10.2307/20041562
- Kightlinger M.F., *Twilight of the idols? EU internet privacy and the post enlightenment paradigm*, „Columbia Journal of European Law” 2007, Vol. 14, No. 114.
- Kissinger H., Schmidt E., Huttenlocher D., *The age of AI: and our human future*, London 2022.
- Kusche I., *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, „Journal of Risk Research” 2024, DOI: 10.1080/13669877.2024.2350720.
- Lane J., Potok N., *Democratizing data: our vision*, <https://hdrs.mitpress.mit.edu/pub/m1o4oblm/release/1>.
- Lizak R., *Prawne aspekty neuronowego modelu zarządzania danymi w administracji federalnej Stanów Zjednoczonych z wykorzystaniem AI*, Warsaw 2024.
- Lizak R., *Redukcja inflacji prawa z wykorzystaniem AI w Stanach Zjednoczonych na tle raportu Dragiego dla Unii Europejskiej*, „Kortowski Przegląd Prawniczy” 2025, No. 4.
- Manzuik S., Gold A., Gatford C., *Network security assessment*, <https://lira.epac.to/DOCS-TECH/Security/Network%20Security/Network%20Security%20Assessment%20-%20From%20Vulnerability%20to%20Patch.pdf>.
- Mayer-Schönberger V., Cukier K., *Big data: a revolution that will transform how we live, work, and think*, Boston 2013.
- McFadden W.C., *Dual-use technologies and national security*, [in:] C.W. Wessner (ed.), *International friction and cooperation in high-technology development and trade: papers and proceedings*, Washington 1997.
- Nowakowski W., *Wykorzystanie sztucznej inteligencji przez małe i średnie firmy w Europie*, [in:] T. Doligalski, D. Kaszyński (eds.), *Sztuczna inteligencja w przedsiębiorstwach i gospodarce (AI SPRING 2024)*, Warsaw 2025.
- Schmidt E. (chair), *Final report. National Security Commission on Artificial Intelligence*, March 1, 2021.
- Wachter S., Mittelstadt B., Floridi L., *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, „International Data Privacy Law” 2017, Vol. 7, Issue 2.
- Zuboff S., *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, London 2019.

Strategic competitiveness between the EU and the United States in artificial intelligence development – human capital, legal frameworks and data

Summary

This article analyzes the level of strategic competitiveness of the European Union and the United States in the development of artificial intelligence based on three key factors determining the development of this technology: the availability of human capital, the regulatory environment, and access to data. The analysis is based on M. Draghi's Report on the competitiveness of the European economy, which is compared with US federal law and strategic documents of the US administration. The article reviews selected legal acts and public documents regulating the development of AI in both jurisdictions, with particular emphasis on the EU AI Act, the GDPR, and selected US federal laws regarding data management and AI development policy. The analysis found that the EU regulatory model focuses primarily on the protection of fundamental rights and risk management related to the use of AI, while the US approach places a greater emphasis on supporting technological innovation, public-private sector collaboration, and broad access to data. Consequently, a more flexible legal environment in the United States promotes the faster commercialization of AI technologies and strengthens their competitive advantage. The article also presents recommendations for strengthening the EU's potential in the area of human capital, simplifying regulation, and increasing the availability of data for the development of AI systems.

Keywords: artificial intelligence, Draghi Report, European Union law, federal law, strategic competitiveness

Strategiczna konkurencyjność między Unią Europejską a Stanami Zjednoczonymi w rozwoju sztucznej inteligencji – kapitał ludzki, ramy prawne i dane

Streszczenie

W artykule podjęto analizę dotyczącą strategicznej konkurencyjności Unii Europejskiej i Stanów Zjednoczonych w rozwoju sztucznej inteligencji na podstawie trzech kluczowych czynników determinujących rozwój tej technologii: dostępności kapitału ludzkiego, otoczenia regulacyjnego oraz dostępu do danych. Punktem odniesienia dla analizy jest raport M. Draghiego, dotyczący konkurencyjności gospodarki europejskiej, zestawiony z regulacjami prawa federalnego Stanów Zjednoczonych oraz dokumentami strategicznymi administracji amerykańskiej. W artykule dokonano przeglądu wybranych

aktów prawnych i dokumentów publicznych regulujących rozwój AI w obu systemach prawnych, ze szczególnym uwzględnieniem EU AI Act, RODO oraz wybranych ustaw federalnych Stanów Zjednoczonych dotyczących zarządzania danymi i polityki rozwoju sztucznej inteligencji. W toku analizy ustalono, że model regulacyjny UE koncentruje się przede wszystkim na ochronie praw podstawowych i zarządzaniu ryzykiem związanym z wykorzystaniem AI, podczas gdy podejście amerykańskie kładzie większy nacisk na wspieranie innowacji technologicznych, współpracę sektora publicznego z prywatnym oraz szeroki dostęp do danych. W konsekwencji bardziej elastyczne otoczenie prawne w Stanach Zjednoczonych sprzyja szybszej komercjalizacji technologii AI i wzmacnia ich przewagę konkurencyjną. Artykuł przedstawia również rekomendacje dotyczące wzmocnienia potencjału UE w obszarze kapitału ludzkiego, uproszczenia regulacji oraz zwiększenia dostępności danych dla rozwoju systemów sztucznej inteligencji.

Słowa kluczowe: prawo federalne, prawo Unii Europejskiej, raport Draghiego, strategiczna konkurencyjność, sztuczna inteligencja