SPRAWY MIĘDZYNARODOWE

2025, t. 78, nr 4
ISSN 0038-853X
e-ISSN 2720-0361
DOI 10.35757/SM.2025.78.4.07

JOANNA KULESZA
University of Lodz
ORCID: 0000-0003-0390-6062
joanna_kulesza@wpia.uni.lodz.pl

Europe's Regulatory Sovereignty in the Age of Artificial Intelligence

A Human-Centric Response to the US-China Technological Rivalry

Regulacyjna suwerenność Europy w erze sztucznej inteligencji

Humanocentryczna odpowiedź na rywalizację technologiczną USA i Chin

Keywords:
European Union, EU, artificial intelligence, AI, regulatory sovereignty, US-China rivalry, international law, data governance, rule of law

Słowa kluczowe:
Unia Europejska, UE, sztuczna inteligencja, SI, suwerenność regulacyjna, rywalizacja USA-Chiny, prawo międzynarodowe, zarządzanie danymi, praworządność

Europe's Regulatory Sovereignty in the Age of Artificial Intelligence: A Human-Centric Response to the US-China Technological Rivalry

In an era marked by intensifying US-China rivalry over artificial intelligence, the European Union seeks to position itself as a global regulatory power by advancing a human-centric model of AI governance. This article examines the EU's emerging regulatory framework – most notably the *Artificial Intelligence Act* – as a potential normative and geopolitical instrument. Drawing on theories of normative power, regulatory internationalism, and global governance, the paper explores the extent to which the EU may influence global technological standards through legal and institutional mechanisms. Through comparative policy analysis and selected empirical case studies, it argues that although Europe lacks the technological scale of the United States or China, its evolving regulatory approach appears to offer an alternative trajectory in global AI governance, oriented toward ethics, human rights, and democratic values.

Regulacyjna suwerenność Europy w erze sztucznej inteligencji. Humanocentryczna odpowiedź na rywalizację technologiczną USA i Chin

W dobie narastającej amerykańsko-chińskiej rywalizacji w dziedzinie sztucznej inteligencji Unia Europejska stara się zaznaczyć swoją pozycję jako globalny prawodawca, promując model zarządzania SI zorientowany na człowieka. Artykuł analizuje ramy regulacyjne UE, koncentrując się na *Akcie o sztucznej inteligencji* jako narzędziu normatywnym, które rodzi skutki geopolityczne. W oparciu o koncepcję władzy normatywnej oraz teorię międzynarodowego i globalnego zarządzania badany jest potencjał UE do kształtowania globalnych standardów technologicznych poprzez instrumenty prawne. Analiza porównawcza polityk publicznych oraz studiów przypadków pozwala stwierdzić, że mimo braku porównywalnego do USA i Chin potencjału technologicznego Europa z sukcesem proponuje odmienny model regulacyjny, stanowiący trzecią drogę globalnego zarządzania SI, która opiera się na etyce, prawach człowieka i wartościach demokratycznych.

Introduction

The 21st century has seen the emergence of a digital cold war wherein global powers compete for leadership in transformative technologies, none more pivotal than artificial intelligence (AI). AI is increasingly recognised as central to economic growth, national security, and technological sovereignty, and its development has become a strategic priority for the United States, China, and the European Union. While the US and China dominate the global AI landscape through massive investments and technological capacity, their approaches reflect contrasting models, market-driven innovation in the US and state-led deployment in China. The EU, lacking comparable technological infrastructure, has adopted a distinctive strategy: positioning itself as a global leader in AI governance and regulation.

In this evolving contest, the EU seeks to assert its normative influence through a human-centric approach that prioritises ethical values, democratic principles, and fundamental rights. At the heart of this strategy lies the *Artificial Intelligence Act* (AI Act), a legislative initiative that classifies AI systems according to risk levels and embeds legal obligations around transparency, accountability, and safety. The Act aims not only to protect EU citizens but also to project a regulatory model that can shape global standards – similar to the precedent set by the General Data Protection Regulation (GDPR). In doing so, the EU aspires to redefine technological leadership not merely in terms of innovation output, but in terms of governance quality and legitimacy.

The question that this paper asks is: To what extent can the European Union's regulatory sovereignty in AI translate into effective global normative influence, despite its limited technological capacity? It hypothesises that the EU's human-centric model functions less as a demonstration of technological power than as a mechanism of regulatory diplomacy. The author examines the EU's regulatory model, highlighting its ambition to balance technological development with fundamental rights and the rule of law. Rather than offering a detailed comparison with US or Chinese frameworks, the analysis foregrounds the EU's normative distinctiveness and its potential for international influence. Methodologically, the research adopts a qualitative and interdisciplinary approach, combining legal analysis, sectoral case studies, and stakeholder perspectives. A close reading of EU legal texts, regulatory proposals, and academic

literature provides the foundation for this inquiry, which is situated within the broader context of international AI governance.

To assess the practical implications of the EU's approach, the paper explores three sectoral domains: healthcare, finance, and biometric surveillance, selected for their high relevance to AI application and their ethical complexity. These case studies illustrate the challenges and opportunities posed by a risk-based, rights-oriented regulatory framework. In doing so, the paper evaluates the extent to which the EU's model can foster trustworthy AI while maintaining its global normative ambitions in an increasingly competitive technological environment.

As such, this article is directly relevant to the field of international relations, as it interrogates the interplay between technology governance and global power projection. It examines how the EU's strategy in regulating AI through its AI Act constitutes a novel form of regulatory diplomacy, thereby expanding the conceptual terrain of power in international relations theory beyond material capabilities to include normative and institutional influence. The AI Act represents a rights-based, human-centric governance model that explicitly incorporates ethical values such as transparency, accountability, and fundamental rights into the legislative framework – marking a departure from the predominantly market-oriented or authoritarian models prevalent elsewhere. In doing so, the EU leverages what scholars have termed its normative power to shape the global discourse and standards surrounding emerging technologies.

The article makes an original contribution on three levels. Theoretically, it enriches existing debates on Europe's normative power and regulatory hegemony by demonstrating how law and ethics are deployed as instruments of global influence in the AI domain. Methodologically, it adopts a qualitative, interdisciplinary approach that combines legal-institutional analysis with sectoral case studies and stakeholder perspectives. Empirically, it offers an in-depth examination of the EU's AI Act and its projected impact through illustrative case studies in healthcare, finance, and biometric surveillance – sectors selected for their salience in both technological application and ethical stakes.

Rather than providing a comparative evaluation of the US and Chinese regulatory systems, the paper concentrates on the EU's distinctive model, assessing its potential to set global norms and the practical challenges it faces in doing so. Through this focus, the paper advances a critical under-

standing of how regulatory frameworks can operate as geopolitical tools in an increasingly fragmented digital order. It positions the EU's AI governance not merely as internal policymaking, but as a strategic endeavour with implications for the international distribution of normative authority in cyberspace.

Methodological approach

This article adopts a qualitative, interpretive-legal and comparative methodology aimed at examining the European Union's evolving framework for artificial intelligence governance. The analysis proceeds through a doctrinal reading of key EU legal and policy instruments – primarily the AI Act, the GDPR, and related communications from the European Commission, the European Parliament, and the Council – supplemented by relevant academic literature in international law, political science, and digital governance. The study interprets these texts not only as legal instruments but also as expressions of the EU's broader normative and strategic ambitions in the digital domain.[1]

The research design is comparative, contrasting the EU's regulatory model with those of the United States and China. The comparative scope has been defined according to two principal criteria: regulatory salience – that is, the jurisdictional relevance and global influence of each model – and ethical complexity, meaning the degree to which AI deployment in each context raises normative questions related to privacy, accountability, and human rights. The EU is examined as the paradigmatic instance of a rules-based, rights-oriented model; the US represents a decentralised, market-driven framework; and China illustrates a state-centred, control-oriented approach. This triadic comparison allows for identifying structural divergences in how governance, ethics, and innovation are balanced across political systems.[2]

Empirically, the paper relies on document analysis of official EU legislative proposals, implementation reports, and sector-specific regulatory

1 R. Cryer [et al.], *Research Methodologies in EU Law and International Law*, Oxford University Press, Oxford 2011, p. 45–47.

2 P. Craig, G. de Búrca, *EU Law. Text, Cases, and Materials*, 7th ed., Oxford University Press, Oxford 2020, p. 127–131.

documents, particularly in the fields of healthcare, finance, and biometric surveillance. These sectors were selected because they combine high regulatory salience with significant ethical implications, making them critical testing grounds for the EU's AI governance model. The analysis focuses on how normative principles – such as transparency, fairness, and accountability – are operationalised within sectoral regulatory frameworks, and how these mechanisms reflect the EU's broader pursuit of regulatory sovereignty and normative power in global digital governance.[3]

Analytical framework

This paper adopts a layered analytical framework linking the European Union's normative ambitions to its regulatory practice and global influence. It proceeds from the conceptual foundation of normative power – the EU's capacity to project its values externally through law and regulation[4] – towards the operational notion of regulatory sovereignty, which denotes the Union's exercise of strategic autonomy in defining and enforcing standards for emerging technologies. Within this continuum, the AI Act functions as the institutional mechanism through which normative power is translated into sectoral regulation, mediating between ethical principles and market realities. The subsequent comparative case studies (healthcare, finance, and biometric surveillance) illustrate how these principles are concretised within specific policy domains. Finally, the analysis turns to the global diffusion of EU norms, examining how regulatory sovereignty, once internalised through law, generates external effects via the Brussels effect and transnational interdependence.[5] In this way, the paper situates the EU's AI governance as both an expression of its internal normative order and a vehicle for shaping global digital rulemaking.

3 M. Dawson, *The Governance of EU Fundamental Rights*, Cambridge University Press, Cambridge 2017 (Cambridge Studies in European Law and Policy), p. 175–179.

4 I. Manners, *Normative Power Europe: A Contradiction in Terms?*, "Journal of Common Market Studies" 2002, vol. 40, No. 2, p. 235–258.

5 H. Farrell, A. L. Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, "International Security" 2019, vol. 44, No. 1, p. 42–79; A. Bradford, *The Brussels Effect. How the European Union Rules the World*, Oxford University Press, Oxford 2020, p. 157–163.

Europe's normative singularity in AI regulation

The European Union seeks to establish itself as a normative power, that is, an actor whose global influence derives primarily from its capacity to project values through legal and institutional means rather than from economic or military coercion.[6] This concept emphasises the Union's ability to shape the behaviour of others through the diffusion of norms – particularly democracy, human rights, and the rule of law – thus distinguishing it from traditional realist understandings of power.[7] Within the digital domain, this normative aspiration manifests itself through regulatory instruments designed to embed ethical principles into technological governance.

This strategic focus is embodied in two key legal instruments: the GDPR and the AI Act. Both reflect the EU's commitment to rights-based, transparent, and accountable digital governance, emphasising human dignity and autonomy in algorithmic systems. They also show how the EU uses its internal market rules to project influence beyond its borders, as other states and companies adopt these standards to access the European market.

Recent scholarship has reinterpreted this dynamic through the lens of the Brussels effect, a term coined by Anu Bradford to describe the EU's unilateral capacity to externalise its regulatory standards beyond its borders through market mechanisms.[8] This phenomenon stresses how the EU's normative power operates through law and commerce rather than diplomacy or coercion. At the same time, scholars such as Henry Farrell and Abraham L. Newman argue that this capacity to export rules is designed as a new form of weaponised interdependence, in which regulatory power becomes an instrument of structural influence within global networks of data and trade.[9] In this sense, the EU's regulatory activism in cyberspace is both defensive (protecting citizens and values), and strategic (asserting global normative leadership).

6 I. Manners, *Normative...*

7 Idem, *The European Union's Normative Power. Critical Perspectives and Perspectives on the Critical*, [in:] *Normative Power Europe*, ed. R. G. Whitman, Palgrave Macmillan, London 2011 (Palgrave Studies in European Union Politics), p. 230.

8 A. Bradford, *The Brussels...*

9 H. Farrell, A. L. Newman, *Weaponized...*

Complementing this normative approach, the concept of regulatory sovereignty captures the EU's pursuit of strategic autonomy in digital governance, understood as the ability to determine its own regulatory conditions in a technologically dependent environment.[10] In the context of AI governance, regulatory sovereignty functions as a mechanism of geopolitical self-assertion: by defining ethical and legal parameters for AI development, the EU seeks to balance technological lag with normative leadership. The AI Act thus embodies not merely a legal instrument but a manifestation of the Union's ambition to shape the moral and institutional architecture of global AI governance.[11]

Since 2018 the GDPR has played a significant role in establishing the EU as a leader in global data governance. By imposing rigorous compliance standards on entities processing the data of EU citizens, the GDPR set a high bar for data privacy and user rights, influencing legal frameworks far beyond Europe. Its extraterritorial reach had a profound impact, compelling businesses and governments worldwide to reassess their data privacy practices and policies. Building upon the GDPR's legacy, the EU introduced the AI Act in 2021.[12] This legislation aims to create a harmonised legal framework for artificial intelligence across EU member states. At its core, the AI Act seeks to promote human-centric AI by proposing a risk-based classification system, wherein AI applications are regulated in proportion to their potential societal impact. The Act categorises AI systems into four levels of risk – unacceptable, high, limited, and minimal – and imposes corresponding regulatory requirements. Unacceptable risk systems, such

10 *Rethinking Strategic Autonomy in the Digital Age*, European Commission, [Brussels] 2019 (EPSC Strategic Notes, 30), p. 14.

11 L. Floridi, *Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical*, "Philosophy & Technology" 2019, vol. 32, No. 1, p. 190–191; *Getting the Future Right: Artificial Intelligence and Fundamental Rights*, European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg 2020.

12 *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) 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)* [hereinafter: AI Act], "Official Journal of the European Union", L 2024/1689, 12 VII 2024.

as those that enable social scoring or exploit vulnerabilities, are prohibited outright. High-risk systems, including those used in critical domains such as healthcare, education, and law enforcement, must meet strict transparency, accountability, and human oversight requirements. Limited- and minimal-risk systems face lighter obligations, ensuring that innovation is preserved while maintaining essential safeguards.[13]

A central principle of the AI Act is proportionality, meaning regulatory requirements reflect the level of risk. This approach allows for more freedom to innovate in low-risk areas while ensuring more thorough oversight in sensitive domains. For example, high-risk AI systems must undergo rigorous documentation, risk assessments, and human supervision. In contrast, lower-risk systems face simpler transparency rules. The Act also mandates regular audits to address algorithmic bias and discrimination, aiming to promote fairness and protect vulnerable populations.

Transparency is another cornerstone of the EU's regulatory framework.[14] High-risk AI systems are required to provide detailed documentation to ensure that decision-making processes are explainable and challengeable. This is particularly crucial in areas such as healthcare, where algorithmic outputs can significantly impact individuals' lives. These transparency measures are designed to foster public trust in AI technologies and ensure their ethical deployment.

The EU's values-based approach contrasts sharply with the models adopted in the United States and China. The US approach, characterised by a largely *laissez-faire* attitude, emphasises market-driven innovation over comprehensive regulation. While initiatives like the *National Artificial Intelligence Initiative Act* and the *Artificial Intelligence Risk Management Framework* represent steps toward AI oversight, they remain largely voluntary and sector specific.[15] This model has been criticised for inadequately

13 M. L. Mueller, *It's Just Distributed Computing: Rethinking AI Governance*, "Telecommunications Policy" 2025, vol. 49, No. 3, p. 154–155.

14 P. Radanliev, *AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development*, "Applied Artificial Intelligence" 2025, No. 39, p. e2463722-1–e2463722-41: <https://www.tandfonline.com/doi/epdf/10.1080/08839514.2025.2463722?needAccess=true> [accessed: 31 VII 2025].

15 *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, National Institute of Standards and Technology, U.S. Department of Commerce, 2023 (NIST AI 100-1): <https://doi.org/10.6028/NIST.AI.100-1> [accessed: 31 VII 2025].

addressing issues of fairness, discrimination, and transparency. In contrast, China's approach is marked by centralised, state-driven regulation[16]. Chinese authorities regard AI development as a crucial component of national strategic goals, embedding ethical guidelines within a broader political framework that reinforces state control.[17] Regulations such as the *Internet Information Service Algorithm Recommendation Management Provisions* prioritise political stability, social control, and alignment with party ideology, diverging sharply from the EU's emphasis on individual rights and the rule of law.[18]

Situated between these two poles, the EU seeks to provide a third way that protects fundamental rights while supporting technological innovation. However, this regulatory model faces major challenges, including uneven enforcement among member states and the difficulty of keeping pace with the fast-changing global AI landscape. In addition, the extraterritorial application of EU rules creates complex issues for cross-border data flows and regulatory alignment.[19]

The EU's AI Act stands as a pioneering attempt to embed democratic values and human rights into the governance of emerging technologies. As global debates on AI oversight intensify, the EU's approach offers a significant – though debated – model for balancing technological innovation with social responsibility, ethical accountability, and long-term human welfare.

16 R. Creemers, *China's Emerging Data Protection Framework*, "Journal of Cybersecurity" 2022, vol. 8, No. 1.

17 H. Roberts [et al.], *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*, [in:] *Ethics, Governance, and Policies in Artificial Intelligence*, ed. L. Floridi, Springer, Cham 2021 (Philosophical Studies Series, 144).

18 *Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022* "Stanford Cyber Policy Center DigiChina" [online], 10 I 2022 [accessed: 31 VII 2025]: <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>; J. Li [et al.], *Honor the Contract? Effects of Algorithmic Recommendation System Features on Perceived Benefits, Privacy Risk, and Continuance Intention to Use TikTok*, "International Journal of Human–Computer Interaction" 2024, vol. 41, No. 17, p. 10713–10724: <https://doi.org/10.1080/10447318.2024.2436736> [accessed: 31 VII 2025].

19 M. Smuha, *From a "Race to AI" to a "Race to AI Regulation": Regulatory Competition for Artificial Intelligence*, "Law, Innovation and Technology" 2021, vol. 13, issue 1, p. 11–13.

Human-centric AI: ethical foundations and risk frameworks

At the core of the European Union's regulatory framework for AI lies a commitment to fundamental human rights. This approach emphasises the importance of individual autonomy and institutional accountability in technological development. Human-centric AI places the well-being of individuals at the centre of governance structures, ensuring that AI systems operate within the legal boundaries established by human rights and societal norms. The objective is to ensure that artificial intelligence technologies are not implemented in ways that undermine individual autonomy or reinforce structural inequalities.[20]

The EU's AI Act formalises this human-centric approach. As the first legislative proposal of its kind on the global stage, the AI Act seeks to establish clear guidelines for the authorisation, use, and oversight of AI systems, while ensuring that risk is minimised without stifling innovation. A key element of the Act is its risk-based classification system, which categorises AI systems into four levels based on the potential harm they may cause. Each category comes with a set of regulatory obligations that increase alongside the level of risk. High-risk systems, such as those deployed in healthcare, employment, and law enforcement, must meet strict requirements of transparency, human oversight, and technical documentation. These obligations ensure that the functions of such systems are traceable, auditable, and open to external review. Lower-risk artificial intelligence systems are subject to less stringent regulatory obligations yet must still comply with fundamental transparency and record-keeping requirements.

Another critical feature of the AI Act is the post-market monitoring requirements for high-risk systems. These systems must undergo continuous evaluation after deployment, with performance data submitted regularly to regulators. If these systems deviate from their intended use or produce harmful outcomes, the Act empowers authorities to intervene and enforce corrective actions, including suspending the operation of such systems. This seeks to ensure that AI technologies remain compliant with ethical and regulatory standards throughout their lifecycle.

The AI Act also addresses issues of fairness, accountability, and transparency. To mitigate potential biases, the Act requires AI systems

20 *Getting the Future...*, p. 11–15.

to undergo audits and impact assessments, especially in sensitive areas such as credit scoring or automated hiring. It holds developers, deployers, and users accountable for ensuring that AI systems function as intended and do not cause harm. Transparency requirements are also strict, with developers required to provide clear documentation and explanations of the algorithms and data used in AI systems. This helps ensure that the decision-making processes behind AI systems are understandable and challengeable by affected individuals and oversight bodies.

In addition, the AI Act aligns with the GDPR, ensuring that privacy is a key consideration in the design and implementation of AI systems. Systems that process personal data must implement measures such as data minimisation, anonymisation, and strong access controls to protect individuals' privacy. These provisions ensure that AI systems do not infringe on the fundamental rights of individuals, particularly in contexts where AI technologies rely on large-scale data collection.

The EU's regulatory model is also notable for its emphasis on stakeholder participation. Policymakers have engaged a wide range of stakeholders, including academics, civil society groups, and industry representatives, in consultations and expert panels to refine the regulatory framework. This inclusive process has helped identify potential implementation challenges and calibrate enforcement mechanisms, ensuring that the regulations are both effective and legitimate across different sectors and jurisdictions.

This human-centric regulatory model distinguishes the EU from other regions. In the United States, the lack of a unified federal framework has resulted in a fragmented regulatory landscape, with varying levels of oversight across sectors. In China, the government's approach to AI is driven by national strategic goals and centralised control. The EU, in contrast, offers a middle ground, balancing technological development with robust institutional oversight and rights-based constraints.

Balancing regulation and innovation

One of the key debates surrounding the European Union's approach to AI regulation is its potential impact on global competitiveness. While much attention is given to the internal effects of regulation, such as the compliance burdens faced by startups and small-to-medium enterprises, it is

equally important to consider the EU's position relative to other major powers, notably the United States and China. These two countries have adopted distinct approaches to AI governance, which contrast with the EU's model. The US favours a decentralised and sectoral approach, while China pursues a state-driven regulatory framework.[21] The EU, on the other hand, has introduced a more structured, rules-based system. This section explores the implications of these differing approaches, particularly in terms of global economic and geopolitical dynamics.

The US approach to AI regulation is largely decentralised, with various federal agencies issuing guidelines in their respective domains. This flexibility allows for rapid innovation but often leads to gaps in accountability and a lack of uniform standards. The absence of a comprehensive national framework creates legal uncertainty for businesses, particularly those engaging in cross-border transactions. In contrast, China's model is characterised by centralised state control, with the government playing a significant role in directing AI development in line with national priorities. This top-down approach prioritises social stability, national security, and alignment with political objectives, which can limit innovation in certain areas.

The EU's model offers a different path. Through the AI Act, the EU establishes a consistent, legally binding framework that imposes clear obligations on developers, deployers, and users of AI systems. These include requirements for documentation, testing, and monitoring, which ensure compliance and reduce legal ambiguity. While this model introduces compliance costs, it also provides a level of predictability and stability that may be advantageous for firms, especially when compared to the uncertainty of the US system or the rigidities of the Chinese approach.

The EU's AI regulatory framework represents a deliberate effort to build a values-based system for governing new technologies. It aims to ensure that innovation develops within clear ethical and legal boundaries that protect human dignity, transparency, and fairness. Although the framework faces ongoing challenges – such as keeping pace with rapid technological change and ensuring consistent enforcement across member states – it

21 M. Mueller, *The US-China Cold War in Cyberspace*, "Internet Governance Project" [online], 19 IV 2020 [accessed: 31 VII 2025]: <http://internetgovernance.org/2020/04/19/the-us-china-cold-war-in-cyberspace/>.

marks an important step in linking technology with democratic principles. By setting rules that tie market access to responsible design and oversight, the EU seeks both to safeguard its internal values and to influence the global debate on how artificial intelligence should be governed.

Comparing AI regulation across key sectors

This section examines the regulation of AI across key sectors, highlighting how governance approaches differ between major global actors. Regulatory, ethical, and political contexts shape these differences, leading to distinct models of AI oversight. The analysis focuses on three critical sectors – healthcare, finance, and biometric surveillance – to provide a comparative understanding of how AI is governed in practice. Particular attention is given to the European Union's framework, which is contrasted with the more decentralised regulatory model of the United States and the state-driven approach of China. The discussion aims to assess how these regions manage ethical risks while promoting technological innovation, and how the EU seeks to balance human rights protection with the advancement of AI technologies.

AI in healthcare: balancing risk and privacy

Analytical question: How does the AI Act operationalise the European Union's human-centric principles in the highly sensitive domain of healthcare, and what does this reveal about the Union's approach to technological risk and ethical accountability?

The application of artificial intelligence in healthcare encompasses diagnostic assistance, treatment recommendations, and personalisation of medical care. Given the high-risk nature of these applications, the EU has established a regulatory framework that integrates privacy, transparency, and rigorous conformity assessments as its core pillars. The AI Act classifies most medical AI systems as high-risk, requiring them to undergo strict pre-market evaluations and continuous post-market monitoring.[22] This approach ensures not only technical reliability but also the protection of patient autonomy and data privacy.

22 AI Act, annex III.

Unlike earlier digital policies that primarily addressed data protection (e.g., the GDPR), the AI Act operationalises the EU's human-centric vision of technology by embedding ethical constraints into the very structure of innovation.[23] The requirement for transparency, human oversight, and auditability in healthcare AI systems translates abstract values – such as dignity and accountability – into legal obligations. As studies by EIT Health and Alessandro Mantelero demonstrate, this reflects a deliberate attempt to build trust as a regulatory objective, positioning healthcare AI as both a technological and moral enterprise.[24]

In contrast, the United States' fragmented, sector-specific regulatory approach – dominated by agencies such as the Food and Drug Administration – emphasises effectiveness and safety but lacks a cohesive ethical framework. This results in gaps concerning algorithmic fairness and data transparency.[25] China's centralised, innovation-driven model prioritises rapid technological scaling but provides insufficient safeguards for patient data and consent, undermining public trust.[26] The EU's approach thus reflects its broader normative identity: regulation as a means of embedding ethical responsibility into market structures, rather than constraining innovation.

Notwithstanding these ambitions, overlaps between the AI Act and *Regulation (EU) 2017/745 […] on Medical Devices* (hereinafter: MDR) create interpretive and practical uncertainties regarding classification, conformity

23 L. Floridi, *The Ethics of Artificial Intelligence*, Oxford University Press, Oxford 2022, p. 117–122.

24 *AI and Ethics in the Health Innovation Community*, EIT Health, Brussels 2019, p. 25: <https://eithealth.eu/wp-content/uploads/2020/01/AI-and-Ethics-in-the-Health-Innovation-Community.pdf> [accessed: 31 VII 2025]; A. Mantelero, *Regulating AI within the Human Rights Framework: A Roadmapping Methodology*, [in:] *European Yearbook on Human Rights 2020*, ed. P. Czech [et al.], Intersentia, 2020, p. 477–502.

25 *Artificial Intelligence in Software as a Medical Device*, "U.S. Food and Drug Administration" [online], 25 III 2025 [accessed: 31 VII 2025]: <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device>.

26 W. J. Vogt, *Artificial Intelligence "with Chinese Characteristics:" A New Model for a New Age*, Social Science Research Network, 17 VII 2025: <https://papers.ssrn.com/sol3/Delivery.cfm/5341204.pdf?abstractid=5341204&mirid=1&type=2> [accessed: 31 VII 2025].

assessment, and market surveillance.[27] While the AI Act introduces horizontal obligations for high-risk AI systems, the MDR already imposes specific safety and performance requirements for software with medical functions.[28] The coexistence of these regimes raises questions concerning the delineation of regulatory competence, particularly where AI components are embedded in medical devices subject to dual compliance. In such instances, producers may exploit definitional ambiguities to circumvent certain AI-specific obligations, a concern acknowledged in rec. 62 of *Regulation (EU) 2024/1689*, which emphasises the need for coherent application between the two instruments.[29] These regulatory junctures highlight that the AI Act's effectiveness in healthcare will depend not only on its normative clarity but also on the operational alignment of overlapping EU legal frameworks.

AI in finance: promoting trust

Analytical question: How does the European Union's financial AI regulation institutionalise transparency and accountability, and to what extent does it reflect a governance model distinct from United States and Chinese approaches?

Artificial intelligence plays a crucial role in financial services – ranging from automated credit scoring to fraud detection. In the EU, the AI Act classifies many financial applications as high-risk, requiring conformity assessments and detailed documentation of algorithmic processes.[30] These provisions aim to ensure explainability and accountability, allowing regulators and consumers to understand and contest AI-based decisions.

27 *Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC*, "Official Journal of the European Union", L 117, 5 V 2017.

28 Ibidem, art. 2, annex I, chap. II, sec. 17.

29 Recital 62 of the AI Act uses a complementary example and underscores that, without prejudice to Regulation (EU) 2024/900, AI systems intended to influence the outcome of elections or referenda, or the voting behaviour of natural persons, should be classified as high-risk AI systems, except where their output is not directly exposed to voters (e.g., internal campaign-management tools), thereby highlighting the need for coherent and consistent application of both instruments.

30 AI Act, art. 52–55.

According to the European Banking Authority, the overarching objective is to enhance consumer trust and safeguard financial stability by mitigating algorithmic bias and systemic opacity.[31]

Analytically, the EU's approach reveals a regulatory strategy of anticipatory governance: it intervenes *ex ante* to prevent systemic risks rather than reacting *ex post* to market failures.[32] This differs significantly from the US framework, which relies on a patchwork of agencies (U.S. Securities and Exchange Commission, Federal Reserve, Consumer Financial Protection Bureau) and voluntary guidelines, fostering flexibility but also inconsistency.[33]

China's centralised financial governance model, while effective in scaling fintech applications, is often criticised for subordinating consumer protection to state control and economic objectives.[34]

The EU's financial AI regime thus serves as a test case for the broader Brussels effect in algorithmic governance – where regulatory coherence and ethical framing function as instruments of both market discipline and normative influence.[35]

Biometric surveillance and privacy concerns

Analytical question: To what extent does the Europeans Union's restrictive stance on biometric surveillance express a distinct normative logic of privacy and proportionality, and how does it diverge from United States and Chinese models?

Biometric surveillance, particularly facial recognition, characterises the ethical tension between security and privacy. Under the AI Act, such technologies are designated as high-risk and subject to strict requirements

31 *EBA Report on Big Data and Advanced Analytics*, European Banking Authority, Paris 2020, p. 5, 11–13.

32 V. Mayer-Schönberger, T. Ramge, *Reinventing Capitalism in the Age of Big Data*, Basic Books, New York 2018, p. 94–96.

33 J. C. Crisanto [et al.], *Regulating AI in the Financial Sector: Recent Developments and Main Challenges*, Bank for International Settlements, Basel 2024 (FSI Insights on Policy Implementation, 63), p. 13–15.

34 R. H. Huang, *Fintech Regulation in China. Principles, Policies and Practices*, Cambridge University Press, Cambridge 2021.

35 A. Bradford, *The Brussels...*

of transparency, fairness, and accountability. In certain cases, such as real-time facial recognition in public spaces, the Act imposes outright prohibitions, reflecting the EU's precautionary approach to the protection of fundamental rights.[36]

This approach shows that the EU sees itself as a constitutional regulator of technology. Instead of viewing AI only as a tool for efficiency, the EU governs it through principles of rights and proportionality. Scholars have noted that this legal prudence aligns with the EU's broader jurisprudence on privacy and human dignity, distinguishing it from the more utilitarian and security-oriented practices of other powers.[37]

In the US, the absence of a federal biometric law, save for state-level instruments such as Illinois' *Biometric Information Privacy Act*, results in a fragmented regulatory landscape.[38] In China, biometric technologies are embedded in state-driven systems of social management and public security, raising profound concerns over surveillance and autonomy.[39] In this context, the EU's cautious regulatory model reflects a clear assertion of regulatory sovereignty, seeking to promote privacy as a universal public norm rather than a regional exception to global practices.

Global influence and norm diffusion

The European Union aspires to play a leading role in shaping the governance of emerging technologies, especially AI. Its influence is often described through the Brussels effect, the idea that EU regulations can shape global standards beyond its borders. Through comprehensive frameworks such as the AI Act, the EU aims to address ethical and societal concerns while promoting responsible innovation. However, its ability to influence global practices remains uncertain, as other regions may adopt different approaches.

36 AI Act, art. 5, sec. 1d.

37 S. E. Dorraji, M. Barcys, *Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations*, "Social Technologies" 2014, vol. 4, No. 2, p. 306–317.

38 *Biometric Information Privacy Act*, "Illinois Compiled Statutes", chap. 740 ILCS 14/1 et seq.

39 R. Creemers, *China's Social Credit System and AI Governance*, "Journal of Cyber Policy" 2022, vol. 7, No. 2, p. 112–130.

This section examines how the EU's regulatory model spreads internationally and the limitations it faces in achieving global cohesion.

The EU's regulatory power stems from its substantial economic influence and market size. As one of the world's largest markets, EU regulations, such as the GDPR, have set global benchmarks for data privacy and protection. Similarly, the AI Act is poised to have a similar global impact by setting standards related to transparency, accountability, and fairness in AI governance. Companies outside the EU, seeking access to the European market, may be compelled to adopt these regulatory standards, thereby extending the EU's influence beyond its borders.

Multilateral organisations such as the Organisation for Economic Cooperation and Development (OECD), the Global Partnership on AI, and the G7 play a significant role in facilitating the diffusion of EU norms. Through its participation in these platforms, the EU actively advocates for AI governance principles that reflect its regulatory priorities, including fairness, transparency, and human rights protection.[40] The OECD's AI principles, which were shaped by the EU, have been widely adopted, setting a global standard for ethical AI use.

In addition to multilateral efforts, the EU integrates its AI governance provisions into bilateral trade agreements. By embedding data protection and transparency clauses in trade deals, the EU encourages third-party countries to align their regulatory frameworks with European standards. This integration extends the reach of the EU's regulatory model, fostering the global adoption of its human-centric approach to AI governance.

Despite these efforts, the global adoption of the EU's regulatory framework is not without challenges. Political, economic, and cultural differences may hinder the widespread acceptance of EU-style regulations. For instance, the United States, with its market-oriented approach, may be resistant to the EU's precautionary stance on AI, while China's centralised control model may prioritise its own regulatory priorities. These geopolitical differences could slow the diffusion of EU norms, particularly in regions where the US or China holds significant influence.

40 S. Feldstein, *Evaluating Europe's Push to Enact AI Regulations: How Will This Influence Global Norms?*, "Democratization" 2024, vol. 31, No. 5, p. 1049–1066.

Moreover, the complexities associated with implementing the AI Act, particularly for smaller nations or businesses with limited resources, may pose additional challenges. The stringent requirements of transparency, monitoring, and compliance could be difficult for developing economies to adopt, potentially leading to a divide between regions with the capacity to enforce EU standards and those without.

Despite these barriers, the EU's AI regulations have significant potential to influence global AI governance. Through multilateral and bilateral initiatives, as well as its trade relations, the EU is advancing the global adoption of its ethical standards. While challenges remain, the EU's leadership in AI regulation is expected to offer a model for other regions to follow, advocating for the responsible development and deployment of AI that aligns with fundamental rights and ethical considerations.

Conclusion

The European Union's regulatory framework for AI provides a comprehensive model for addressing the complex ethical and societal challenges posed by AI technologies. Through its emphasis on transparency, accountability, and fairness, the EU aims to position itself as a global leader in AI governance. As global markets continue to grapple with the implications of AI, the EU's approach is expected to influence the future of AI regulation worldwide. By continuing to advocate for human rights and ethical AI standards, the EU aims to ensure that the benefits of AI are realised while mitigating its risks.

The EU's approach to AI regulation is designed as an effort to address the ethical, societal, and legal implications of emerging technologies. The AI Act, with its focus on human rights, transparency, and accountability, seeks to provide a framework that manages AI risks while aligning development with fundamental values. The regulation is intended to include provisions to mitigate algorithmic bias, protect personal data, and address labour displacement, aiming to create an environment where technological progress and public welfare are balanced.

The EU's regulatory framework faces challenges, particularly due to the global divergence in approaches to AI governance. The differences in regulatory frameworks between the United States, China, and other regions may create barriers to international cooperation. This fragmenta-

tion, or so-called splinternet, could result in inefficiencies, as businesses and governments may need to navigate a range of regulations.[41] The EU's ability to promote and sustain cooperation and align standards globally is essential in addressing these issues.

While the EU seeks to establish influence in shaping global norms, especially through its trade relationships and economic power, it must work to overcome resistance from regions with different political and economic priorities.[42] Efforts to promote human-centric AI norms will require continued engagement with international fora, bilateral agreements, and diplomatic channels.

Despite the projected global influence of the AI Act, the diffusion of its standards through the so-called Brussels effect remains subject to structural and jurisdictional limits. The Act's extraterritorial application is bounded by market access logic rather than enforceable global jurisdiction: third-country operators are only bound insofar as they place AI systems on the Union market or affect EU users. Consequently, while the AI Act is expected to shape international best practices, its capacity to impose uniform compliance obligations beyond the EU's regulatory perimeter remains constrained. These limitations illustrate a broader tension between normative ambition and juridical reach, suggesting that the EU's global regulatory power functions primarily through indirect market incentives rather than formal legal authority.[43]

The EU's leadership in AI governance provides an opportunity to set a global standard that prioritises human dignity, ethical considerations, and fundamental rights. To succeed, the EU must continue advocating for international collaboration, push for alignment in AI regulations across borders, and address the social and economic challenges posed by AI. By doing so, the EU seeks to contribute to shaping a global framework that encourages innovation while ensuring responsible and equitable development. Future research should assess, once the AI Act becomes fully

41 L. Schmitt, *Mapping Global AI Governance: A Nascent Regime in a Fragmented Landscape*, "AI and Ethics" 2022, vol. 2, No. 2, p. 303–314.

42 S. Meunier, N. Kalypso, *The European Union as a Conflicted Trade Power*, "Journal of European Public Policy" 2006, vol. 13, No. 6, p. 906–925; S. Lütz [et al.], *European Union as a Global Actor. Trade Finance and Climate Policy*, Springer, Cham 2021.

43 A. Bradford, *The Brussels...*; H. Farrell, A. L. Newman, *Weaponized...*

operational in 2026, whether its normative ambitions translate into effective extraterritorial regulatory impact or remain primarily symbolic.

Bibliography

AI and Ethics in the Health Innovation Community, EIT Health, Brussels 2019: <https://eithealth.eu/wp-content/uploads/2020/01/AI-and-Ethics-in-the-Health-Innovation-Community.pdf> [accessed: 31 VII 2025].

Artificial Intelligence in Software as a Medical Device, "U.S. Food and Drug Administration" [online], 25 III 2025 [accessed: 31 VII 2025]: <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device>.

Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology, U.S. Department of Commerce, 2023 (NIST AI 100-1): <https://doi.org/10.6028/NIST.AI.100-1> [accessed: 31 VII 2025].

Biometric Information Privacy Act, "Illinois Compiled Statutes", chap. 740 ILCS 14/1 et seq.

Bradford A., *The Brussels Effect. How the European Union Rules the World*, Oxford University Press, Oxford 2020.

Craig P., Búrca G. de, *EU Law. Text, Cases, and Materials*, 7th ed., Oxford University Press, Oxford 2020.

Creemers R., *China's Emerging Data Protection Framework*, "Journal of Cybersecurity" 2022, vol. 8, No. 1.

Creemers R., *China's Social Credit System and AI Governance*, "Journal of Cyber Policy" 2022, vol. 7, No. 2.

Crisanto J. C., Leuterio C. B., Prenio J., Yong J., *Regulating AI in the Financial Sector: Recent Developments and Main Challenges*, Bank for International Settlements, Basel 2024 (FSI Insights on Policy Implementation, 63).

Cryer R., Hervey T., Sokhi-Bulley B., Bohm A., *Research Methodologies in EU Law and International Law*, Oxford University Press, Oxford 2011.

Dawson M., *The Governance of EU Fundamental Rights*, Cambridge University Press, Cambridge 2017 (Cambridge Studies in European Law and Policy).

Dorraji S. E., Barcys M., *Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations*, "Social Technologies" 2014, vol. 4, No. 2.

EBA Report on Big Data and Advanced Analytics, European Banking Authority, Paris 2020.

Ethics, Governance, and Policies in Artificial Intelligence, ed. L. Floridi, Springer, Cham 2021 (Philosophical Studies Series, 144).

European Yearbook on Human Rights 2020, ed. P. Czech, L. Heschl, K. Lukas, M. Nowak, G. Oberleitner, Intersentia, 2020.

Farrell H., Newman A. L., *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, "International Security" 2019, vol. 44, No. 1.

Feldstein S., *Evaluating Europe's Push to Enact AI Regulations: How Will This Influence Global Norms?*, "Democratization" 2024, vol. 31, No. 5.

Floridi L., *The Ethics of Artificial Intelligence*, Oxford University Press, Oxford 2022.

Floridi L., *Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical*, "Philosophy & Technology" 2019, vol. 32, No. 1.

Huang R. H., *Fintech Regulation in China. Principles, Policies and Practices*, Cambridge University Press, Cambridge 2021.

Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022 "Stanford Cyber Policy Center DigiChina" [online], 10 I 2022 [accessed: 31 VII 2025]: <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>.

Li J., Chen T., Li S., Hu B. , *Honor the Contract? Effects of Algorithmic Recommendation System Features on Perceived Benefits, Privacy Risk, and Continuance Intention to Use TikTok*, "International Journal of Human–Computer Interaction" 2024, vol. 41, No. 17: <https://doi.org/10.1080/10447318.2024.2436736> [accessed: 31 VII 2025].

Lütz S., Leeg T., Otto D., Dreher V. W., *European Union as a Global Actor. Trade Finance and Climate Policy*, Springer, Cham 2021.

Manners I., *The European Union's Normative Power. Critical Perspectives and Perspectives on the Critical*, [in:] *Normative Power Europe*, ed. R. G. Whitman, Palgrave Macmillan, London 2011 (Palgrave Studies in European Union Politics).

Manners I., *Normative Power Europe: A Contradiction in Terms?*, "Journal of Common Market Studies" 2002, vol. 40, No. 2.

Mantelero A., *Regulating AI within the Human Rights Framework: A Roadmapping Methodology*, [in:] *European Yearbook on Human Rights 2020*, ed. P. Czech, L. Heschl, K. Lukas, M. Nowak, G. Oberleitner, Intersentia, 2020.

Mayer-Schönberger V., Ramge T., *Reinventing Capitalism in the Age of Big Data*, Basic Books, New York 2018.

Meunier S., Kalypso N., *The European Union as a Conflicted Trade Power*, "Journal of European Public Policy" 2006, vol. 13, No. 6.

Mueller M., *The US-China Cold War in Cyberspace*, "Internet Governance Project" [online], 19 IV 2020 [accessed: 31 VII 2025]: <http://internetgovernance.org/2020/04/19/the-us-china-cold-war-in-cyberspace/>.

Mueller M. L., *It's Just Distributed Computing: Rethinking AI Governance*, "Telecommunications Policy" 2025, vol. 49, No. 3.

Normative Power Europe, ed. R. G. Whitman, Palgrave Macmillan, London 2011 (Palgrave Studies in European Union Politics).

Radanliev P., *AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development*, "Applied Artificial Intelligence" 2025, No. 39: <https://www.tandfonline.com/doi/epdf/10.1080/08839514.2025.2463722?needAccess=true> [accessed: 31 VII 2025].

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC, "Official Journal of the European Union", L 117, 5 V 2017.

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) 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), "Official Journal of the European Union", L 2024/1689, 12 VII 2024.

Rethinking Strategic Autonomy in the Digital Age, European Commission, [Brussels] 2019 (EPSC Strategic Notes, 30).

Roberts H., Cowls J., Morley J., Taddeo M., Wang V., Floridi L., *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*, [in:] *Ethics, Governance, and Policies in Artificial Intelligence*, ed. L. Floridi, Springer, Cham 2021 (Philosophical Studies Series, 144).

Schmitt L., *Mapping Global AI Governance: A Nascent Regime in a Fragmented Landscape*, "AI and Ethics" 2022, vol. 2, No. 2.

Smuha M., *From a "Race to AI" to a "Race to AI Regulation": Regulatory Competition for Artificial Intelligence*, "Law, Innovation and Technology" 2021, vol. 13, issue 1.

Vogt W. J., *Artificial Intelligence "with Chinese Characteristics:" A New Model for a New Age*, Social Science Research Network, 17 VII 2025: <https://papers.ssrn.com/sol3/Delivery.cfm/5341204.pdf?abstractid=5341204&mirid=1&type=2> [accessed: 31 VII 2025].