

Regulatory models of artificial intelligence in contemporary governance: Comparative analysis of China, the EU and the USA

Mykhailo Shkilniak^{*1} 

¹Department of Management, Public Administration and Personnel, Western Ukrainian National University, Ternopil, Ukraine

Abstract. The rapid development of artificial intelligence and its penetration into critically important spheres of social life have confronted global governance with unprecedented challenges that require the development of balanced regulatory approaches. The aim of this study was to compare the main regulatory models of artificial intelligence governance in the world's leading regions – China, the European Union and the United States of America – and to identify areas of divergence as well as potential opportunities for mutual influence and adaptation within the contemporary political and ethical context. The research methodology was based on a combination of comparative, analytical and case-study methods. The regulatory frameworks and policies of the EU, the USA and China were analysed, along with case studies from Estonia, the African Union and leading technology corporations, which made it possible to identify differences in approaches to the regulation and practical application of artificial intelligence. The results of the study demonstrated that artificial intelligence has become a strategic resource shaping a new configuration of global power balances. The European regulatory model ensured a comprehensive approach to risk assessment through a multi-level classification of systems. The Chinese model demonstrated the effectiveness of centralised control and rapid scaling, while the American approach retained a fragmented character due to the absence of a single federal law. A trend was identified whereby international organisations play a role in shaping universal ethical standards, yet their capacity to ensure real coordination remains limited. It was found that the European Union's "Brussels effect" contributes to the transnationalisation of European norms, while China and the United States disseminate their own models through digital diplomacy and corporate expansion respectively. Certain countries, such as Estonia, have demonstrated a successful combination of digitalisation of public administration with democratic principles, using cryptographic protection mechanisms and decentralised access to data. The results of the study may serve as a basis for developing adaptive strategies for artificial intelligence governance in countries with different levels of institutional development and may contribute to the formulation of international agreements in the field of digital policy

Keywords: digital sovereignty; cybersecurity; algorithmic governance; digital authoritarianism; social networks; electronic governance; administrative efficiency

INTRODUCTION

The rapid development of artificial intelligence (AI) and its integration into spheres of social life have created a qualitatively new level of challenges for global governance. AI has ceased to be merely a technological tool and has become a strategic resource capable of influencing the balance of power in international relations, economic transformations and social structures. At the same time, the absence of unified approaches to its regulation at the global level has led to policy fragmentation, intensifying geopolitical competition

between states and creating risks of increasing inequality in access to technologies.

Previous studies laid the foundation for understanding the dynamics of AI governance but did not eliminate certain gaps. The study by V.I. Espinosa & A. Pino (2025) focused on the case of Estonia, where e-government based on principles of transparency, trust and security contributed to economic transformation and increased social welfare. The authors demonstrated that the successful integration of the e-government model was made possible by

Suggested Citation:

Shkilniak, M. (2025). Regulatory models of artificial intelligence in contemporary governance: Comparative analysis of China, the EU and the USA. *Journal of Global Political Transformations*, 1(1), 56-68. doi: 10.67524/verus1/1.2025.56.

*Corresponding author



a comprehensive combination of legal and technological innovations. The work of E. Erman & M. Furendal (2024) emphasised that, despite the widespread discourse on “AI governance”, the theoretical basis remained insufficiently developed. The authors pointed to a deficit of procedural legitimacy in existing regulatory models and argued that delegating governance functions to algorithms undermined democratic principles. They proposed a conceptual framework for assessing the legitimacy of global regulatory mechanisms, but the empirical dimension of their model was limited. In the study by I. Ulnicane *et al.* (2022), concepts from social studies of science and technology were applied to explain the formation of AI policies. The authors analysed the role of expectations and competition in new technological sectors, revealing that policies were often the result of interactions between academic communities, governments and corporations. The article by A. Taihagh (2021) emphasised that the rapid development of autonomous systems, particularly for military purposes, created unprecedented governance challenges. The author showed that regulatory frameworks lagged behind technological change and that governments’ institutional capacities remained insufficient.

In the work of R.J. Neuwirth (2024), a shift in emphasis from national to global regulation was proposed. The author argued that, in order to minimise AI-related risks, regulatory discussions must be integrated into the broader context of the UN Sustainable Development Goals. The study considered AI as a factor of cognitive transformation of global governance but did not provide concrete mechanisms for implementing this vision in interstate interaction. The work of R. Radu (2021) presented the first comprehensive analysis of national AI strategies adopted between 2017 and 2019. It demonstrated that most states preferred ethics-oriented approaches rather than legal frameworks, which led to the formation of hybrid governance models. R.B.L. Dixon (2023) proposed a universal governance model based on an analysis of the approaches of China, the USA and the EU. The author identified seven recommendations for integrating ethical principles into policy, drawing attention to vulnerable groups facing the greatest risks. Discussions on effective artificial intelligence governance took place at the intersection of political, ethical and economic dimensions, but their theoretical and practical integration remained limited, highlighting the need for research capable of proposing institutionally and normatively balanced regulatory approaches.

The aim of this study was to conduct a comparative analysis of regulatory approaches to artificial intelligence governance in China, the European Union and the United States of America, with an emphasis on their conceptual differences, ethical orientations and institutional implementation mechanisms. The objectives of the study were to: conduct a comparative analysis of regulatory approaches to artificial intelligence in China, the EU and the USA; identify key challenges and differences between state, supranational and corporate models of AI governance; and

generalise promising directions for mutual influence and adaptation of regulatory practices in order to enhance the ethical nature, transparency and effectiveness of artificial intelligence policies.

MATERIALS AND METHODS

The methodological framework of the study combined comparative, analytical and case-study methods, enabling a systematic analysis of approaches to AI regulation in the world’s leading political and legal systems. The core tool was comparative legal and institutional analysis, through which regulatory frameworks and policy implementation mechanisms in the European Union, the United States of America and China were examined. The main sources included A New Generation of Artificial Intelligence Development Plan (State Council of the People’s Republic of China Document No. 35, 2017), The EU Artificial Intelligence Act (2021), AI Bill of Rights (Blueprint for an AI Bill of Rights, 2022) and the AI Risk Management Framework (2023). For the ethical dimension of the study, the Recommendation on the Ethics of Artificial Intelligence (2023), which defines universal principles for the responsible use of algorithmic systems, was used. Content analysis was conducted through thematic coding of regulatory acts and strategic documents according to the following categories: regulatory framework; institutional governance structure; areas of AI application; ethical and security risks; level of international integration; and manifestations of “soft power”.

Coding was carried out by two researchers using the NVivo software environment, ensuring interpretative consistency (double coding) and systematic organisation of the material. The comparison of characteristics employed thematic matrices in Excel, which made it possible to summarise differences between models according to defined criteria. Document selection criteria included representativeness of models (supranational, national and corporate), relevance (primarily post-2020), the presence of ethical and human rights provisions, and the ability to demonstrate extraterritorial influence – particularly the EU’s “Brussels effect” (Bradford, 2020).

The study also incorporated auxiliary case studies: the African Union (2024) as an example of a collective regional approach; Estonia with its Kratt Strategy and the X-Road – Interoperability services (n.d.) platform as a case of democratic digitalisation; and Turkey, India and Latin America for analysing specific political dynamics in interaction with digital platforms. At the level of corporate practices, the activities of Google (n.d.), Microsoft (n.d.), OpenAI (n.d.), NVIDIA (n.d.), Netflix (n.d.) and TikTok (n.d.) were examined, demonstrating different forms of corporate influence on AI policy.

The theoretical foundation is provided by the concept of “soft power” (Nye, 2004), used to interpret how AI technologies are transformed into instruments of political, economic and cultural influence by states and corporations. The limitations of the study are related to the fact

that the analysis is based on official documents that reflect declared policy rather than actual practice; corporate sources may contain elements of strategic positioning; and different jurisdictions publish documents of varying scope and structure, complicating standardised comparison. Despite this, the chosen approach ensured the comprehensiveness of the analysis and made it possible to identify structural differences between AI regulatory models in the world's leading regions.

RESULTS

Theoretical and conceptual foundations of global governance in the age of AI

The evolution of the concept of global governance reflects a complex process of transformation of the international system, from the dominance of state-centred models to the emergence of multi-level and networked regulatory mechanisms. Whereas classical approaches to global governance focused on the actions of sovereign states, intergovernmental organisations and the system of international law, by the end of the twentieth century a clear trend had begun to take shape towards the inclusion of non-state actors – transnational corporations, international non-governmental organisations and global financial institutions (Nwokike, 2022). The digital age has radically accelerated this process, creating conditions for new forms of power and influence based on control over information flows and data infrastructure. It is during this period that the notion of global governance has gradually been supplemented by the categories of “digital sovereignty”, “cybersecurity” and “algorithmic governance”. Artificial intelligence is one of the most powerful catalysts of this transformation, because it not only expands the toolkit of state and supranational actors, but also changes the very nature of political and administrative practices. In public administration, the deployment of machine-learning algorithms makes it possible to optimise decision-making processes, reduce bureaucratic costs and anticipate societal needs on the basis of “big data” analysis (Bajracharya, 2024). In the political domain, artificial intelligence alters the structure of public communication. Algorithms that drive the operation of digital platforms become new “architects” of political discourse, determining which topics gain public salience and which groups receive greater opportunities to articulate their interests. This, in turn, creates new mechanisms of mobilisation and control that often extend beyond classical democratic procedures. In administrative terms, AI appears as a tool for managerial efficiency. The automation of public-service procedures demonstrates the technology's potential to build transparent and citizen-oriented governance systems (Anshari *et al.*, 2025). Here, algorithms are able not only to process information but also to act as intermediaries between the citizen and the state, reducing bureaucratic barriers and increasing trust in institutions. At the same time, however, risks associated with algorithmic “black boxes” grow: when the logic

of decision-making remains opaque, there is a danger of power being concentrated in the hands of technological elites or private corporations that control the software.

The challenges that arise in the process of integrating artificial intelligence into global governance encompass a set of interconnected problems that have both immediate political and administrative consequences and strategic implications for the international system. One of the most acute issues is the security dimension (Hu *et al.*, 2021). The use of AI in national defence and cyber protection opens new possibilities for developing effective mechanisms for threat detection and attack forecasting. Yet it also raises the problem of autonomous weapons systems that can make decisions without human control. This brings up questions of accountability for the actions of such systems, particularly in cases involving violations of international humanitarian law. An example is the debates surrounding the use of unmanned combat drones in conflicts in the Middle East, where the use of algorithms for target identification is often accompanied by the risk of false positives and civilian casualties (Bornu, 2025). Equally important is the ethical dimension of AI use. Algorithms can reproduce – or even amplify – existing biases embedded in the source data used for training. This is particularly evident in automated recruitment, credit-scoring systems or algorithmic moderation on social networks. For example, studies in the United States have shown that some justice-sector algorithms display a tendency to systematically overestimate the risk of reoffending among African Americans, thereby undermining the principle of equality before the law. Another defining challenge is inequality of access to technology. The gap between technologically advanced countries and states of the Global South intensifies the problem of asymmetry in global governance. Regions lacking adequate infrastructure and investment in AI development risk being excluded from the processes of shaping new rules and standards. For instance, African countries depend on importing ready-made digital platforms created in the United States or China, effectively creating a new form of “digital coloniality” (Akıner, 2024). This constrains their ability to influence the international agenda while also creating risks of dependence on foreign technology corporations. Thus, unequal access becomes not only a socio-economic issue but also a geopolitical factor (Costa, 2023).

At the same time, despite numerous challenges, the application of artificial intelligence in global governance opens up significant potential for addressing supranational problems. These include optimising responses to climate change, monitoring the spread of epidemics, managing migration flows and ensuring food security. In these areas, machine-learning technologies can process data volumes that traditional methods could not analyse and provide states with tools for strategic decision-making at the global level. Table 1 systematises the main challenges and opportunities associated with the use of AI in global governance.

Table 1. Key challenges and opportunities of AI use in global governance

Issue dimension	Key challenges	Examples	Potential opportunities	Examples
Security	Autonomous weapons systems without adequate oversight; cyber threats and algorithmic attacks	Use of combat drones in Syria; AI-enabled cyberattacks in Europe	Development of predictive analytics systems for national security and cyber defence	AI systems for detecting cyberattacks in the EU; forecasting terrorist threats in the USA
Ethics	Algorithmic bias; privacy violations; discrimination in access to services	Risk-assessment systems in the USA that discriminated against African Americans	Development of international standards for ethical AI use	UNESCO “Recommendation on the Ethics of AI”; the EU AI Act
Inequality of access	Digital coloniality; lack of infrastructure in developing countries	Africa and South Asia dependent on importing US and Chinese platforms	Technology transfer programmes; international co-operation in AI	African AI development strategy; UN digital inclusion initiatives
Global problems	Lack of co-ordination in regulation; risk of fragmentation of international rules	Divergent models: EU AI Act; absence of a single law in the USA; state control in China	Use of AI to address supranational challenges	UN climate-change monitoring systems; AI-supported analysis of COVID-19 spread

Source: compiled by the author based on Y. Hu *et al.* (2021), The EU Artificial Intelligence Act (2021), Recommendation on the Ethics of Artificial Intelligence (2023), S. Costa (2023), African Union (2024), M. Basu & M.D. Nath (2024), T.Z. Bornu (2025), R. Arslan *et al.* (2025)

An analysis of the table shows that artificial intelligence is simultaneously a source of threats and a powerful resource for improving the effectiveness of global governance. The most critical are security risks linked to autonomous weapons systems and cyber threats, as these can extend beyond the scope of traditional international law. Ethical challenges create the need to develop universal norms that would regulate algorithm use and guarantee the protection of human rights. Inequality of access clearly demonstrates that the digital divide between countries can entrench new forms of global hierarchy, in which leading states and corporations become the primary centres of power. At the same time, the opportunities opened by AI are no less significant: from creating predictive-analytics systems for security to developing global strategies for responding to climate and humanitarian challenges. This indicates that the task of the international community is to balance risk minimisation with maximising AI's potential, which requires co-ordination at the level of international organisations, harmonisation of regulatory frameworks and the development of inclusive co-operation programmes.

In international relations, artificial intelligence is increasingly viewed not only as a technological tool or an economic resource, but also as a powerful driver of “soft power”. The concept of “soft power”, proposed by J.S. Nye (2004), rests on a state's ability to influence other countries through the attractiveness of its culture, political values and institutions, rather than through coercion or economic pressure. Artificial intelligence, given its universal and global character, becomes a new dimension of this category, as it allows states to project their technological standards, cultural narratives and models of digital development onto the international arena. Competition over the right to set regulatory frameworks for AI use is particularly significant in this context. By promoting The EU Artificial Intelligence Act (2021), the European Union is effectively shaping a normative standard that can extend far beyond Europe. This process is often compared to the

so-called “Brussels effect”, whereby EU legal practices become a global norm due to the economic attractiveness of the European market and high requirements for ethics and transparency (Bradford, 2020). In this way, the EU uses AI regulation as an element of its “soft power”, emphasising a commitment to human rights, privacy protection and democratic values. As a result, this supports public trust and the effectiveness of digital services within member states, while also setting standards for the international use of technologies.

China has chosen a different path, treating artificial intelligence as an instrument for promoting a model of digital authoritarianism (Zeng, 2020). Large-scale investments in facial-recognition technologies, social credit systems and control over digital platforms have formed a distinctive governance model that is exported to countries in Africa, Latin America and the Middle East through “digital diplomacy”. For many states seeking effective mechanisms to control social processes, the Chinese experience becomes an attractive template, strengthening Beijing's influence without the need for direct coercion. In effect, technologies become carriers of ideology, and algorithms become instruments for shaping an international image. The United States, in turn, advances its “soft power” through innovation ecosystems and the global leadership of technology corporations. Companies such as Google (n.d.), Microsoft (n.d.), OpenAI (n.d.) and NVIDIA (n.d.) act as “ambassadors” of an American model of AI development based on market principles, open innovation and competitiveness. The export of American software products and research practices creates not only economic dependence but also cultural and value-oriented alignment, as AI technologies are integrated into the everyday practices of millions of users worldwide. An example is the global spread of chatbots built on American models, which not only provide technological functionality but also embed certain standards of communication, language and information interpretation in users' perceptions (Chen *et al.*, 2024).

A distinct vector of using AI as a “soft power” resource is educational and scientific diplomacy. States that invest in international exchange programmes, grants and research laboratories in the AI field effectively build a positive image and expand their circle of partners. Three major centres of power are clearly visible here: China, the USA and the European Union. China actively develops a network of Confucius Institutes with a focus on technological innovation (Flew & Hartig, 2014), while the USA supports numerous Fulbright (n.d.) programmes, in which researchers have opportunities to work on AI-related projects. The European Union, in turn, uses Horizon Europe (n.d.) to fund international research that demonstrates its commitment to global scientific collaboration. All these initiatives correspond to basic selection criteria: representativeness (reaching a global audience), extraterritoriality (creating international research hubs) and human rights (a public declaration of value standards associated with academic freedom).

The cultural dimension of AI within “soft power” manifests itself in control over algorithmic systems that govern global digital platforms. Netflix (n.d.) and TikTok (n.d.) shape a unified cultural agenda through recommendation algorithms that affect the accessibility and popularity of cultural products. Control over a platform means control over global cultural trends: TikTok provides China with an additional channel of influence, while American platforms ensure the USA’s resistant leadership in digital culture. The European Union, unlike the USA and China, seeks to balance these dynamics through regulatory initiatives, where the operationalisation of effectiveness is defined by the level of algorithmic transparency and compliance with human-rights standards in the digital services sphere. Thus, in contemporary international relations, artificial intelligence is a powerful instrument of “soft power” operating on several levels. Regulatory frameworks allow states to spread their values and political models; technology corporations create economic and cultural dependence; educational and scientific programmes generate a positive image; and digital platforms shape global cultural trends. All of this suggests that, in an era of digital transformation, “soft power” ceases to be a purely humanitarian instrument and increasingly rests on technologies, algorithms and innovation ecosystems. The balance between different models of AI use in “soft power” will determine the future character of global governance and the distribution of influence among the world’s leading states.

Examples from regions illustrate how the triad (China – USA – EU) is reflected in local contexts. In Latin America, a key phenomenon has been the dominance of closed messaging services and short-video platforms in political mobilisation (Rincón & Uribe-Rincón, 2024). WhatsApp is used as a grassroots co-ordination network and a channel for disseminating political messages that bypass moderation; mass mailouts and group “meshes” have provided tools for rapid mobilisation and the spread of disinformation, especially during elections in Brazil (Breuer, 2025). The closed nature of these networks

reduces audit possibilities and strengthens “information bubbles” (Adrian *et al.*, 2021). At the same time, TikTok has opened a space for leaders’ direct communication with young people, strengthening the emotional dimension of politics. In Turkey, digital platforms operate under a regime of strict legal control: legislation expands the state’s powers to block content and access data, which – against the backdrop of polarisation – turns social media into a regulated field of communication. This is accompanied by technical instruments of influence and the use of bot networks to manipulate the agenda (Duygu, 2023), resulting in constraints on freedom of speech and forcing the opposition towards underground channels. In India, platforms function in a linguistically and culturally diverse environment with a vast user base. WhatsApp and localised social networks have become spaces both for mass campaigns and for “popular” mobilisation, while encryption has complicated external oversight and stimulated the development of civic fact-checking initiatives (Maréchal *et al.*, 2021). At the same time, the government has increased pressure through the IT Rules (The Information Technology..., 2021), which formalised platforms’ obligations. Studies show the spread of microtargeting and multilingual campaigns, which raise disinformation risks and simultaneously require localised moderation mechanisms (Kazemi *et al.*, 2022).

In summary, several levels of using AI as an instrument of “soft power” can be distinguished: regulatory (the EU sets standards and transparency), cultural (the USA and China promote their own platforms and algorithms), educational and scientific (global exchange programmes and research funding), and mobilisation and communication (Latin America, Turkey and India as regional cases). As a politico-technological factor, digital platforms also generate practical directions for counteraction and adaptation. Effective approaches include combining technical solutions (tools for detecting bot networks, algorithms for identifying co-ordination), regulatory reforms (transparent content-removal procedures, independent appeals mechanisms) and societal interventions (media literacy, localised fact-checking initiatives and partnerships between platforms and civil society) (Antoliš, 2024). In Latin America, projects are already being tested that combine local fact-checking with technical “tiplines” for collecting message samples from WhatsApp; in India and Turkey, initiatives are emerging to adapt interfaces and ad-verification mechanics to linguistic diversity. However, a persistent obstacle is resource asymmetry: technological solutions require access to platform data and analytical capacities, which are often the privilege of the platforms themselves or high-resource actors. Consequently, a policy of transparency and access to aggregated data becomes a central element for academic research and public oversight.

Comparative analysis of the experience of states and international institutions

State practices in applying artificial intelligence in governance differ markedly in terms of strategy, institutional

organisation, funding models and accountability mechanisms – ranging from centralised plans and strong state direction to a “state as purchaser” model and initiatives based on partnerships with the private sector. For example, the Chinese approach is characterised by a high level of centralised strategic planning, a clear state orientation towards technological dominance, and intensive integration of AI into the security sector and urban management (Allen, 2019). The official A New Generation of Artificial Intelligence Development Plan (State Council of the People’s Republic of China Document No. 35, 2017) set time-bound goals and priorities up to 2025 and 2030, defining state investment, the creation of national research centres and clusters, and a system of incentives for private actors. In practice, this has resulted in large-scale public funding programmes for research, the establishment of industrial parks and preferential support for companies capable of delivering large-scale solutions in the public sector. Within this strategy, AI deployment in urban governance and mass-surveillance instruments has become a standard showcase for efficiency and technical capability; at the same time, such integration has driven the development of algorithmic control and profiling systems, strengthening the state’s capacity for preventive governance while creating challenges for transparency and privacy protection. One element of the Chinese model is the rapid translation of scientific advances into applied systems at provincial and municipal level, accompanied by substantial public procurement and close co-operation between local administrations and major technology firms (Lin, 2025). A practical embodiment of China’s state-industrial model is the “City Brain” project in Hangzhou (Caprotti & Liu, 2022), which combined large volumes of sensor data, telecom data and urban information systems with computer-vision and traffic-optimisation algorithms. Following a pilot launch in 2016, the system reportedly demonstrated concrete improvements in traffic flow and congestion reduction, strengthening the case for scaling the project and exporting the technology to other cities (including international projects). However, techno-economic successes have been accompanied by questions about data control, the terms of public-private partnerships and the long-term creation of a platform for monitoring civic activity – i.e. the “price of transparency” society pays for speed and efficiency. In administration on this scale, the absence of clear mechanisms for external auditing of algorithmic decisions increases the risks of abuse and erroneous decisions in critical situations. Operationalisation of metrics here is based on techno-economic indicators (traffic, response speed), while mechanisms of external audit and human-rights protection remain weak – reflected in the “transparency and human rights” criterion. Representativeness is ensured through scale (coverage of megacities), and extraterritoriality through exporting technologies to third countries.

The Estonian case demonstrates a practically antagonistic model: a state that prioritises digitalisation as a service-oriented transformation aimed at improving the

transparency, accessibility and efficiency of public services while preserving legal safeguards and an architecture of decentralised access to data (Lillemets, 2023). Unlike a model centred on centralised control, the Estonian approach is based on infrastructure solutions – for example, X-Road – Interoperability services (n.d.) for secure data exchange between state registers – alongside “one-stop shop” principles for citizens and mandatory cryptographic protection of transactions. At the policy level, Estonia adopted national strategies aimed at creating ethical, human-centred AI – such as the Kratt Strategy (New e-Estonia fact-sheet..., 2020) – which combine the rollout of practical public-sector solutions (bureaucracy chatbots, tax-fraud detection systems, natural-resource monitoring) with an emphasis on algorithmic openness, workforce training and international co-operation. Specific cases, such as the Bürokratt chatbot network or computer-vision systems for environmental monitoring, illustrate an effort to deliver measurable benefits to citizens (reduced time to access services, improved anomaly-detection accuracy) without abandoning legal certainty and auditability (Kaun & Männiste, 2025). This balance is achieved through standardised interfaces, open APIs and clear auditing protocols, which reduce barriers to oversight by both the public and independent institutions.

The US model differs from both of the above through the dominance of the private sector as innovator and solution provider, alongside fragmented federal regulation. Recent federal initiatives have focused on developing standards, guidance and risk-governance frameworks – such as the AI Risk Management Framework (2023) – seeking to establish a technical and administrative basis for safe and ethical AI use without imposing direct, strict regulation on development as such. The US approach is more inclined towards instruments that incentivise innovation and experimentation (pilot programmes, grants, partnerships with universities), while also paying attention to guidance on accountability, verification and safety testing. At the political level, framework documents have emerged – for example, Blueprint for an AI... (2022) – which outline citizens’ rights in the age of automated systems; on the other hand, regulatory behaviour may shift depending on the administration and political direction, creating uncertainty for long-term investment in responsible practices. The set of American approaches includes active use of public procurement to shape market standards, the encouragement of open research ecosystems and close co-operation with industry leaders to develop testing and certification methods. Metrics are operationalised through risk-management and audit indicators, as well as through research on trust in technologies (Anderson *et al.*, 2023).

The effectiveness of AI implementation in public administration depends not only on the technical sophistication of systems but also on the presence of risk-control mechanisms: procedures for assessing impacts on human rights, standards for algorithmic audits, requirements for data transparency and contractual conditions in public

procurement. Here, Estonia is an example of formalising such mechanisms at an early stage, whereas in the US projects combine technical risk-management frameworks with voluntary industry initiatives; China, meanwhile, faces issues of external oversight and international legitimacy. Given technological dynamics, political will and international constraints, an optimal national strategy requires hybrid solutions: clear strategy and investment (as in China), an orientation towards rights, inclusiveness and openness (as in Estonia), and support for an innovation-oriented ecosystem (as in the US), but with much stronger international mechanisms for co-ordination and the harmonisation of baseline standards (Parisini, 2025).

With regard to evaluating outcomes, practical indicators of effectiveness should include a set of quantitative and qualitative metrics: service delivery time and automation error rates for public services; changes in security indicators and response speed in the event of critical incidents for urban-management systems; the number of recorded and addressed cases of bias or unlawful data use; and levels of public trust, measured through regular surveys and independent audits. Constructing such metrics requires a multidisciplinary approach (law, ethics, computer science, sociology) and the creation of regulatory frameworks for transparent reporting on effectiveness. In this sense, national initiatives to develop risk-governance standards (including NIST (National Institute of Standards and Technology) frameworks) and guidance on citizens' rights (for example, the AI Bill of Rights) form a basis for such assessments and can serve as reference points for adapting local policies. Comparative analysis shows that each model has clear advantages and structural limitations. China's centralised model enables rapid scaling and synergy of national resources, but it is more vulnerable to risks of authoritarian use and reduced transparency; the Estonian model shows that combining digital infrastructure with principles of openness and human rights delivers resistant operational outcomes for citizens, but scaling it in larger and politically more diverse states may be constrained by institutional and resource limitations; the American model stimulates innovation and the emergence of global technology leaders, but the lack of a coherent regulatory field creates risks of inequality, unregulated experimentation and problems of standards interoperability internationally. These differences directly affect which instruments states choose: centralised procurement and national platforms; modular service architectures with open-source components; or combinations of state incentives and corporate innovation.

Regulatory frameworks in the field of artificial intelligence in the twenty-first century constitute one domain of global governance, because it is through legal and ethical norms that it is determined how new technologies are integrated into political, economic and social processes. The European Union, the United States and UNESCO are leading centres for developing such approaches, but each pursues a distinct logic of normative design and strategic positioning. This generates both competition for dominance

in standard-setting and a need to develop minimal global conventions that could ensure compatibility and mutual recognition of regulatory frameworks. The European Union demonstrates the most systematic and ambitious approach to building legal norms for AI, embodied in the preparation and adoption of The EU Artificial Intelligence Act (2021). This legal instrument, for the first time in world practice, creates a comprehensive classification of AI systems by risk level – from “minimal” to “unacceptable”. The latter category includes practices such as social scoring used for total control over citizens, as well as real-time biometric identification except in clearly defined cases. A distinctive feature of the AI Act is its emphasis on preventive control and certification of technologies at the stage of their development. In this way, the EU seeks to implement a “regulation through risk” logic that combines the protection of human rights with innovation competitiveness. The law has an extraterritorial character: any company seeking access to the European market must comply with its requirements.

The American approach is far more fragmented and pragmatic, which is explained by both political culture and the structure of public administration in the United States. Unlike the EU, Washington has not created a single codified AI law; instead, regulation is carried out through a combination of “soft law”, sectoral standards and strategic initiatives. A central place in this system is occupied by Blueprint for an AI... (2022), published by the White House in 2022. This document is not legally binding, but it provides a framework for protecting citizens' rights in the age of algorithms, emphasising principles such as transparency, non-discrimination, the ability to opt out of automated decisions and the right to an explanation. In parallel, the United States is actively developing guidance from the NIST, in particular the AI Risk Management Framework (2023), which aims to establish a unified approach to assessing and mitigating risks associated with algorithmic use. UNESCO's initiatives in AI have a different character, as the organisation does not possess coercive instruments comparable to state laws and instead develops global framework norms and recommendations. In 2021, the Recommendation on the Ethics of Artificial Intelligence (2023) was adopted, becoming the first comprehensive global document oriented towards ethical standards for AI use. This instrument is based on four fundamental principles: respect for human rights, inclusiveness, sustainable development and the promotion of peace. The emphasis is on preventing the deepening of inequalities, given the risk that countries with limited resources will remain outside the development process for new technologies. UNESCO insists on the need to develop national strategies that take into account not only technical but also cultural, social and educational features. In addition, the organisation's recommendations are aimed at establishing mechanisms of transparency, accountability and access to technology for countries of the Global South. This makes UNESCO's initiatives a compensatory factor countering asymmetry between technological giants and less developed states.

In summary, these three approaches reflect different models of global governance. The EU seeks to establish strict legal standards underpinned by its economic strength and ability to project norms beyond its jurisdiction. The United States develops a decentralised, innovation-oriented regulatory model in which the private sector plays the leading role and the state provides only framework guidance. UNESCO, in turn, offers a universalist, value-driven approach that attempts to balance the interests of different groups of actors and to give voice to less

developed countries. At the same time, these approaches are not only in competition but also complementary: UNESCO's recommendations can provide a basis for global discussions; American flexibility supports the speed of innovation; and European legal norms protect human rights and democratic values. In the longer term, the synthesis of these three vectors may become the foundation for creating a truly effective and fair system of global AI regulation. A more detailed comparison of these regulatory models is presented in Table 2.

Table 2. Regulatory models of AI use in different regions

Parameter/ Region	European Union (AI Act)	United States (federal initiatives and voluntary standards)	China (state strategy and regulatory initiatives)	UNESCO (Recommendation on the Ethics of AI)
Policy objective	Protection of fundamental rights, prevention of harm; establishment of unified legal standards for the EU market	Promotion of innovation and competitiveness while mitigating risks; establishing principles without mandatory, unified codification	National technological leadership; economic and security uses of AI; accelerated commercialisation and meeting state needs	Development of ethical and legal guidance, universal principles (respect for human rights, inclusiveness, sustainable development)
Legal status and binding force	Codified law (entered into force); mandatory requirements for high-risk systems; bans on unacceptable practices	Predominantly "soft law": executive documents (Executive Orders), NIST guidance, frameworks without mandatory federal sanctions	Combination of directives, technical standards and sectoral rules; strong role of executive power and administrative acts; rapid issuance of norms based on strategic plans	Intergovernmental recommendations endorsed by member states; no direct coercive force, but commit to implementing principles in national policies
Approach to risk and scope	Risk-based: classification of systems (minimal-limited-high-unacceptable); mandatory conformity assessment for high-risk	Framework and risk-management orientation (NIST AI RMF) with voluntary application; focus on risk-management processes across the life cycle	Pragmatic, industry-oriented classification: priorities include security, information control, public-order management; operational restrictions for specific uses (e.g. chatbots, deepfakes) via specific administrative acts	Ethical approach: principles for assessing impacts on human rights, transparency requirements, responses to inequalities; call for national impact assessments
Implementation instruments	Certification/conformity assessment, documentation requirements, mandatory human-in-the-loop/control in some applications; fines and administrative sanctions	Public procurement as an incentive, R&D grants, publication of guidance; sectoral codes, voluntary audits; separate state-level laws	Centralised public R&D funding programmes, public procurement, priority industrial clusters; administrative guidance on content moderation and data localisation	Technical assistance to countries, methodological tools for national strategies, audit and impact-assessment guidance; promotion of education and inclusive programmes
Accountability mechanisms	Supervisory authorities (national AI bodies, audits), mandatory registration of high-risk systems, fines; extraterritorial effect via market access	Political and administrative oversight, sectoral regulators in specialised areas; public and market pressure	Administrative control, operational instructions for providers, co-operation with security services/police; limited public audit due to control of the information environment	Monitoring of implementation through member-state reporting mechanisms; recommendations on institutional mechanisms for implementation
Transnational action/extraterritoriality	Clear extraterritorial effect (market impact – non-EU firms must comply)	Smaller extraterritorial effect; greater reliance on private-sector co-operation and voluntary international standards	Bilateral technology agreements, export of platforms and solutions; practical impact via infrastructure projects (digital export)	Orientation towards global uptake of principles; focus on developing countries; no coercive extraterritoriality, but offers a standard ethics model
Impact on innovation and business ecosystem	Standardisation may raise entry barriers for smaller actors, but promotes "trustworthy AI" and creates market advantage for certified products	Flexibility supports rapid innovation cycles and corporate leadership, but risks "regulatory arbitrage"	State stimulates industry through investments and public contracts; rapid scaling model, but with risks of market centralisation around key players	Support for inclusive innovation policies, grant and educational assistance to strengthen capacity in low-resource regions

Table 2. Continued

Parameter/ Region	European Union (AI Act)	United States (federal initiatives and voluntary standards)	China (state strategy and regulatory initiatives)	UNESCO (Recommendation on the Ethics of AI)
Human-rights and inequality safeguards	Strong emphasis on fundamental rights; inadmissibility of social scoring; privacy protection	Rights focus via non- binding guidance (AI Bill of Rights), but implementation depends on sectoral standards	Priority on security and public order; human rights present in documents, but implementation often subordinated to state interests; risks of rights restrictions	Human rights and preventing the deepening of inequalities are central; call for technology-transfer and access policies

Source: compiled by the author based on G.C. Allen (2019), The EU Artificial Intelligence Act (2021), Blueprint for an AI... (2022), AI Risk Management Framework (2023), Recommendation on the Ethics of Artificial Intelligence (2023), X. Lin (2025), E. Parisini (2025)

The regulatory models presented in the table reflect three main logics of state AI policy: rights-oriented (EU), innovation-market (USA) and state-industrial (China), complemented by a universalist ethical framework (UNESCO). These logics are shaped by a combination of political priorities, institutional capacity and economic interests. A shared feature is that all approaches recognise the need for risk governance, protection of certain rights and the creation of trust in technologies, but they differ in the preferred means: legal bans and certification (EU), voluntary technical frameworks and market incentives (USA), state programmes and control of access/content (China), and international ethical co-ordination (UNESCO). The existence of a strong “Brussels effect” means that the EU acts as a catalyst for global standard harmonisation through its market weight and extraterritorial requirements on suppliers. This creates a practical need for American and Chinese companies to adapt products to European norms, while also generating tension between economic efficiency and legal compliance. The American model, in the absence of a single strict law, encourages rapid diffusion of innovation, but this can complicate the establishment of unified global standards without active international co-operation. China’s strategy shows that state co-ordination enables rapid scaling of applications, but creates barriers to adopting international ethical norms where they conflict with national interests. UNESCO’s recommendations serve as a balancing element, offering general principles for international dialogue and support for less developed countries.

Prospects for global co-ordination depend on three practical conditions. First, the need to develop a minimal “international package” of binding norms protecting basic rights (for example, banning total social scoring and establishing minimum transparency guarantees for systems that affect people’s lives). Such a package could be negotiated intergovernmentally and based on UNESCO principles, but should include implementation mechanisms (for example, cross-border agreements or mutual recognition of certificates). Second, institutional mechanisms for technical co-operation are needed: joint test environments for model evaluation, workable formats for algorithmic audits and standardised metrics for impacts on human rights and security. This would require the involvement of independent organisations, intergovernmental institutions and academic

centres. Third, asymmetry must be addressed: financially and technically weaker countries must gain access to funding, technology transfer and capacity building, to avoid repeating a “digital coloniality” scenario. UNESCO and regions with strong standards (the EU) can serve as sources of such support programmes. Concrete practical recommendations to initiate co-ordination include establishing a multi-stakeholder technical certification centre, developing a basic “black-and-white” classification of unacceptable practices (agreed by most countries), and implementing technical-assistance mechanisms for Global South countries (grants to create national AI audit institutions). At national level, this implies combining elements of all models: risk-based legislation (as in the EU), innovation incentives (as in the USA) and state co-ordination of strategic directions (as in China), but with mandatory human-rights safeguards and transparent audit procedures. From a research perspective, further studies should focus on the empirical measurement of each model’s effectiveness: comparative studies of the impact of regulatory decisions on innovation indicators (patents, investment), human rights (complex indicators of discrimination and violations) and market competitiveness. Practical steps for the research community include developing replicable methods for algorithmic audits, political-economy models for assessing extraterritorial regulatory effects, and sets of indicators for evaluating “implementation readiness” in low-resource countries.

DISCUSSION

In the discussion dimension of the study, it was important to compare the findings with previous scholarly work, which made it possible not only to identify the consonance of conceptual approaches but also to delineate differences in interpretations of artificial intelligence as an instrument of global governance and as a source of political and legal transformation. In F. Filgueiras (2022), emphasis was placed on the early stage of AI policy formation, which was examined through the lens of policy and governance regimes. The typology proposed by the author helped to explain the dynamics of interaction between actors, institutions and ideas that determined the strategic vectors of national approaches. Unlike the present study, which demonstrated that AI has already become a catalyst for a fundamental transformation of global governance

and has contributed to new centres of power, F. Filgueiras focused on a formative stage in which the main contours of political regimes were only beginning to take shape. Conclusions about the dual nature of AI policy – between technological development and regulatory instruments – correlated with the divergence between the Chinese, European and American models identified in this research. At the same time, a key difference is that this analysis emphasised geopolitical consequences and the emergence of algorithmic governance as a new form of power, whereas Filgueiras treated the issue primarily through an institutional and normative lens. J. Zeng's (2022) monograph provided a comprehensive analysis of the phenomenon of "AI with Chinese characteristics", revealing the multi-layered nature of Beijing's approach. The author argued that China's strategy was not limited to centralised geopolitical steering, but was to a significant extent shaped by economic actors and exhibited bottom-up features. This position contrasted with the conclusions of the present study, in which the Chinese model was described as an instrument of centralised governance with high risks for human rights. Common ground remained the recognition that Chinese specificity has shaped a new variety of digital authoritarianism, capable of combining the effectiveness of technological solutions with the securitisation of society. At the same time, this analysis indicated that the success of China's strategy depended on achieving a balance between economic growth, social stability and ideological control, which aligned with the present study's thesis about AI being used as a tool of geopolitical power and as a vehicle for exporting authoritarian practices. However, the present study emphasised the foreign-policy dimension and the global diffusion of "digital authoritarianism", whereas J. Zeng focused on domestic political and economic determinants.

In E. Erman & M. Furendal (2025), the principal emphasis was on the role of non-state actors in legitimising global AI governance. The authors distinguished two analytical dimensions – "democratic agents" and "agents of democracy" – arguing that transnational corporations have insufficient legal grounds for the former status but considerable moral and market authority for the latter. Compared with these conclusions, the findings of the present study revealed a more critical dependence of the global architecture on corporate structures, which not only performed auxiliary or indirect functions but in practice shaped the contours of international policy. This was evident in the US case, where the absence of a single federal legislative framework delegated a significant share of regulatory and innovation processes to corporations. Thus, whereas in Erman and Furendal corporate participation was viewed as potentially legitimised through moral and epistemic authority, the present study's results pointed to a deeper structural dependence of national models on corporations, creating additional challenges for democratic accountability.

B. Neupane (2024) focused on the integration of AI and big data into public-administration processes, emphasising

efficiency, transparency and scalability through cloud environments. It was illustrated that such technologies enabled a new level of responsiveness and resource optimisation, while being accompanied by privacy risks and ethical dilemmas. Comparison with the present study's conclusions showed that similar opportunities have indeed been realised in governance practices, particularly in China and Estonia, where digital administration systems demonstrated high effectiveness in public services. The difference lay in emphasis: whereas B. Neupane interpreted digital transformation primarily as a technological and operational shift, the present study highlighted its geopolitical dimension, in which technologies became resources for strategic competition and factors reshaping the international balance of power. Thus, shared features in assessments of AI's potential for public administration were confirmed, while a more complex political and security configuration of its use was also underscored. S. Mokry & J. Gurol (2024) emphasised that global initiatives to regulate AI have become not only normative instruments but also means of geopolitical competition. The authors stressed that China, the USA and the EU sought to position themselves as leaders in AI governance, and that the process of global co-ordination proved subordinate to a logic of competition for influence. This conclusion resonated with the present study's findings, which developed the idea that algorithmic governance is gradually forming new centres of power and that AI technologies are becoming instruments of "soft power". At the same time, this analysis showed that international institutions, including the UN and UNESCO, have been insufficiently effective in harmonising divergent approaches, whereas S. Mokry & J. Gurol primarily emphasised the competitive nature of regulatory initiatives and the risks of fragmentation. A further distinction was this study's emphasis on empirical examples – such as China's "City Brain" programme or the European AI Act – demonstrating concrete mechanisms through which AI is transformed into an instrument of power.

In H. Roberts *et al.* (2023), a comparative analysis of Chinese and European models identified the key difference as a gap between Beijing's innovation-economic focus and Brussels' ethical-legal emphasis. The authors concluded that closing regulatory gaps would require mutual borrowing of the strengths of both approaches. This logic aligned with the present study's conclusions, which likewise stressed divergence between China's centralised model and Europe's rights-protecting model. At the same time, the present analysis situated the issue in a broader context: AI was defined not merely as an object of innovation or regulation, but as a catalyst for the formation of new global hierarchies of power. The difference lay in scale of interpretation: whereas H. Roberts *et al.* limited themselves to recommendations for bilateral improvement, the present study demonstrated the geopolitical consequences of technological rivalry and AI's role in reshaping the architecture of the international order. R.B.L. Dixon (2022) systematised more than ninety AI

governance initiatives formulated by various governmental, private, academic and multilateral structures. On this basis, the author identified fundamental AI principles intended to underpin the development of coherent policy recommendations. This approach corresponded with the present study's findings in recognising the importance of multi-level interaction between state and non-state actors. However, whereas R.B.L. Dixon emphasised the search for universal principles and the possibility of forming a globally coherent governance system, the present analysis suggested the opposite dynamic: global regulation remains fragmented, and international institutions do not demonstrate sufficient effectiveness. Another distinct emphasis of this study was the role of AI as a strategic resource of geopolitical influence, whereas Dixon prioritised conceptualising ethical and legal principles. In summary, all the works reviewed supported the thesis that AI regulation extends far beyond technical or administrative tasks and has become part of broader political and geopolitical processes. This allowed the conclusion that contemporary dynamics of AI regulation combine elements of pragmatic competition and ideological confrontation with attempts to identify universal principles; however, it is the geopolitical dimension that appears decisive in shaping the architecture of the future global order.

CONCLUSIONS

The study illustrated that artificial intelligence has become a catalyst for a fundamental transformation of global governance, shifting from a technological tool to a strategic resource of geopolitical influence. This is reflected in the emergence of new centres of power, a rethinking of the concept of digital sovereignty, and the rise of algorithmic governance as a new form of exercising power. A comparative analysis of national approaches in China, the EU and the USA revealed deep divergence in their regulatory philosophies: the Chinese model demonstrated the effectiveness of centralised state steering and rapid technological scaling in projects such as "City Brain" in Hangzhou, but with significant human-rights risks through social credit systems and mass surveillance; the European approach developed the most comprehensive rights-protecting regulatory system through the 2021 AI Act, combining preventive risk control with a four-tier classification of AI systems; the American strategy retained a fragmented, innovation-oriented

character, assigning a substantial role to private corporations in the absence of a single federal law, instead relying on the "Blueprint for an AI Bill of Rights" and the NIST "AI Risk Management Framework" as voluntary guiding principles. The study also found that AI technologies have become powerful instruments of "soft power": China exports a model of "digital authoritarianism" through digital diplomacy initiatives in African and Latin American countries; the EU offers a normative model grounded in the protection of human rights and democratic values; and the USA projects its innovation ecosystem through the global dominance of technology corporations.

The paper further concludes that existing international institutions (the UN and UNESCO) have proved insufficiently effective in harmonising such divergent approaches, contributing to fragmentation of global regulation and rising geopolitical tension in the context of US-China technological confrontation. At the same time, the experience of certain countries, notably Estonia, demonstrated the feasibility of combining a high level of digitalisation (via the X-Road interoperability platform and the "Kratt" strategy) with adherence to democratic principles and human rights through mechanisms of transparency, decentralised data access and cryptographic protection. The study is limited by its comparative focus on only three actors (China, the EU and the USA) and their strategies, which does not fully capture the dynamics of global AI governance, including the role of smaller states, international organisations and under-resourced private actors. Future research prospects include deeper analysis of the empirical consequences of implementing specific regulatory models, the development of mechanisms for adapting AI governance frameworks to developing countries, and the exploration of possibilities for creating new hybrid institutions for global co-ordination under conditions of technological hegemony.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

- [1] Adrian, T., Ferati, E., Gates, I., Liu, L., Mendoza, K., Potnis, S., Schenk, Z., Srinivas, A., & Zachary, T. (2021). *Misinformation in global media: Causes, consequences, and accountability*. Seattle: Henry M. Jackson School of International Studies University of Washington
- [2] African Union. (2024). *Continental artificial intelligence strategy: Harnessing AI for Africa's development and prosperity*. Addis Ababa: African Union.
- [3] AI Risk Management Framework. (2023). Retrieved from <https://www.nist.gov/itl/ai-risk-management-framework>.
- [4] Akiner, N. (2024). *A theoretical approach to the digital colonialism in the context of media imperialism*. In *7th International conference on social science research* (pp. 131-141). Durres: ICONSR.
- [5] Allen, G.C. (2019). *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security*.

- [6] Anderson, M., Faverio, M., & Gottfried, J. (2023). *Teens, social media and technology 2023: YouTube, TikTok, Snapchat and Instagram remain the most widely used online platforms among U.S. teens*. Retrieved from <https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/>.
- [7] Anshari, M., Hamdan, M., Ahmad, N., & Ali, E. (2025). Public service delivery, artificial intelligence and the sustainable development goals: Trends, evidence and complexities. *Journal of Science and Technology Policy Management*, 16(1), 163-181. doi: 10.1108/JSTPM-07-2023-0123.
- [8] Antoliš, K. (2024). Disinformation supported by artificial intelligence from dynamic research to holistic solutions. *Public Security and Public Order*, 35, 11-23. doi: 10.13165/PSPO-24-35-02.
- [9] Arslan, R., Özseven, T., & Aydın, M.M. (2025). Transforming European cybersecurity: AI-powered threat analysis, quantum age, blockchain/crypto risks, and regulatory strategies. *International Journal of Engineering and Applied Sciences*, 17(2), 81-93. doi: 10.24107/ijeas.1619600.
- [10] Bajracharya, K. (2024). *Big data and artificial intelligence integration in modernizing governance and public administration practices*. *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*, 8(12), 34-47.
- [11] Basu, M., & Nath, M.D. (2024). *A study of the role of artificial intelligence in monitoring environmental and health issues in the post-COVID-19 pandemic era for sustainable living*. In X. Savarimuthu, S. Subramani & A.N.J. Raj (Eds.), *Artificial intelligence for multimedia information processing: Tools and applications* (pp. 132-166). Boca Raton: CRC Press.
- [12] Blueprint for an AI Bill of Rights. (2022). *The White House*. Retrieved from <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>.
- [13] Bornu, T.Z. (2025). The challenge of artificial intelligence in the middle east conflicts. *The American Journal of Political Science Law and Criminology*, 7(05), 115-129. doi: 10.37547/tajpslc/Volume07Issue05-14.
- [14] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford: Oxford University Press.
- [15] Breuer, A. (2025). *From polarisation to autocratisation: The role of information pollution in Brazil's democratic erosion*. Bonn: German Institute of Development and Sustainability (IDOS). doi: 10.23661/idp2.2025.
- [16] Caprotti, F., & Liu, D. (2022). Platform urbanism and the Chinese smart city: The co-production and territorialisation of Hangzhou City Brain. *GeoJournal*, 87(3), 1559-1573. doi: 10.1007/s10708-020-10320-2.
- [17] Chen, T., Gascó-Hernandez, M., & Esteve, M. (2024). The adoption and implementation of artificial intelligence chatbots in public organizations: Evidence from US state governments. *The American Review of Public Administration*, 54(3), 255-270. doi: 10.1177/02750740231200522.
- [18] Costa, S. (2023). *Artificial intelligence: Ethical and political challenges*. Santos Costa.
- [19] Dixon, R.B.L. (2022). *Artificial intelligence governance: A comparative analysis of China, the European Union, and the United States*. (Professional paper, University of Minnesota Twin Cities, Minneapolis, MN).
- [20] Dixon, R.B.L. (2023). A principled governance for emerging AI regimes: Lessons from China, the European Union, and the United States. *AI and Ethics*, 3, 793-810. doi: 10.1007/s43681-022-00205-0.
- [21] Duygu, U. (2023). *Between politics and social media: Examining domestic information operations through the Twitter controversy in Türkiye*. (Master's thesis, Sabancı University, Istanbul, Türkiye).
- [22] Erman, E., & Furendal, M. (2024). Artificial intelligence and the political legitimacy of global governance. *Political Studies*, 72(2), 421-441. doi: 10.1177/00323217221126665.
- [23] Erman, E., & Furendal, M. (2025). The democratic role of non-state actors in the global governance of artificial intelligence. *Critical Review of International Social and Political Philosophy*, 1-26. doi: 10.1080/13698230.2025.2520037.
- [24] Espinosa, V.I., & Pino, A. (2025). E-Government as a development strategy: The case of Estonia. *International Journal of Public Administration*, 48(2), 86-99. doi: 10.1080/01900692.2024.2316128.
- [25] Filgueiras, F. (2022). Artificial intelligence policy regimes: Comparing politics and policy to national strategies for artificial intelligence. *Global Perspectives*, 3(1), article number 32362. doi: 10.1525/gp.2022.32362.
- [26] Flew, T., & Hartig, F. (2014). *Confucius institutes and the network communication approach to public diplomacy*. *The IAFOR Journal of Asian Studies*, 1(1), 1-18.
- [27] Fulbright (n.d.). Retrieved from <https://fulbright.org.ua/uk/>.
- [28] Google. (n.d.). Retrieved from <https://www.google.com/?hl=uk>.
- [29] Horizon Europe. (n.d.). Retrieved from https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
- [30] Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2021). Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys*, 55(1), 1-36. doi: 10.1145/3487890.
- [31] Kaun, A., & Männiste, M. (2025). Public sector chatbots: AI frictions and data infrastructures at the interface of the digital welfare state. *New Media & Society*, 27(4), 1962-1985. doi: 10.1177/14614448251314394.
- [32] Kazemi, A., Garimella, K., Shahi, G.K., Gaffney, D., & Hale, S.A. (2022). *Research note: Tiplines to uncover misinformation on encrypted platforms: A case study of the 2019 Indian general election on WhatsApp*. Retrieved from <https://surl.li/ybdztz>.

- [33] Lillemets, P. (2023). *Estonia – a digital government in digital transformation*. (Master's thesis, Tallinn University of Technology, Tallinn, Estonia).
- [34] Lin, X. (2025). A model of big data-based governance: China's national government big data platform and an analysis of its governance competence. *Chinese Political Science Review*, 10, 289-328. doi: 10.1007/s41111-025-00279-1.
- [35] Maréchal, N., Renieris, E., Rydzak, J., Hartmann, I.A., Obar, J.A., Gaur, A., Macpherson, L., Karanicolas, M., & Keton, A. (2021). *Tackling the 'fake' without harming the 'news': A paper series on regulatory responses to misinformation*. Wikimedia/Yale Law School Initiative on Intermediaries and Information.
- [36] Microsoft Dynamics 365. (n.d.). Retrieved from <https://www.microsoft.com/uk-ua/microsoft-365>.
- [37] Mokry, S., & Gurol, J. (2024). Competing ambitions regarding the global governance of artificial intelligence: China, the US, and the EU. *Global Policy*, 15(5), 955-968. doi: 10.1111/1758-5899.13444.
- [38] Netflix. (n.d.). Retrieved from <https://www.netflix.com/tr-en/>.
- [39] Neupane, B. (2024). *Artificial intelligence and big data technologies to optimize government decision-making processes in cloud-based environments*. *Journal of Artificial Intelligence and Machine Learning in Cloud Computing Systems*, 8(11), 1-12.
- [40] Neuwirth, R.J. (2024). The global institutional governance of AI: A four-dimensional perspective. *International Journal of Digital Law and Governance*, 1(1), 113-153. doi: 10.1515/ijdlg-2024-0004.
- [41] New e-Estonia factsheet: National AI "Kratt" strategy. (2020). Retrieved from <https://e-estonia.com/new-e-estonia-factsheet-national-ai-kratt-strategy/>.
- [42] NVIDIA. (n.d.). Retrieved from <https://www.nvidia.com/en-us/drivers/>.
- [43] Nwokike, L.I. (2022). *The rising profile of international non-governmental organizations and their roles in contemporary concept of international governance*. *International Journal of Law and Clinical Legal Education*, 3, 161-171.
- [44] Nye, J.S. (2004). Soft power. *Foreign Policy*, 80, 153-171. doi: 10.2307/1148580.
- [45] OpenAI. (n.d.). Retrieved from <https://openai.com/>.
- [46] Parisini, E. (2025). Governing artificial intelligence in the defence sector: A comparative analysis of EU and US institutions. *Global Public Policy and Governance*, 5, 114-138. doi: 10.1007/s43508-025-00115-x.
- [47] Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society*, 40(2), 178-193. doi: 10.1080/14494035.2021.1929728.
- [48] Recommendation on the Ethics of Artificial Intelligence. (2023). UNESCO. Retrieved from <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>.
- [49] Rincón, O., & Uribe-Rincón, C. (2024). Political communication in Latin America. In A. Casero-Ripollés & P.C. López-López (Eds.), *The Routledge handbook of political communication in Ibero-America* (pp. 19-31). London: Routledge. doi: 10.4324/9781003388937.
- [50] Roberts, H., Cows, J., Hine, E., Morley, J., Wang, V., Taddeo, M., & Floridi, L. (2023). Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. *The Information Society*, 39(2), 79-97. doi: 10.1080/01972243.2022.2124565.
- [51] State Council of the People's Republic of China Document No. 35 "A New Generation of Artificial Intelligence Development Plan". (2017, July). Retrieved from http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.
- [52] Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, 40(2), 137-157. doi: 10.1080/14494035.2021.1928377.
- [53] The EU Artificial Intelligence Act. (2021). Retrieved from <https://artificialintelligenceact.eu/>.
- [54] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. (2021). Retrieved from <https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf>.
- [55] TikTok. (n.d.). Retrieved from <https://www.tiktok.com/uk-UA/>.
- [56] Ulnicane, I., Knight, W., Leach, T., Stahl, B.C., & Wanjiku, W.G. (2022). Governance of artificial intelligence: Emerging international trends and policy frames. In M. Tinnirello (Ed.), *The global politics of artificial intelligence* (pp. 29-55). Boca Raton: CRC Press. doi: 10.1201/9780429446726-2.
- [57] X-road – interoperability services. (n.d.). Retrieved from <https://e-estonia.com/solutions/interoperability-services/x-road/>.
- [58] Zeng, J. (2020). Artificial intelligence and China's authoritarian governance. *International Affairs*, 96(6), 1441-1459. doi: 10.1093/ia/iaa172.
- [59] Zeng, J. (2022). *Artificial intelligence with Chinese characteristics: National strategy, security and authoritarian governance*. Singapore: Palgrave Macmillan Singapore. doi: 10.1007/978-981-19-0722-7.