V International Scientific and Technical Conference Actual Issues of Power Supply Systems

Legal Regulation of Artificial Intelligence in the Energy Sector: A Comparative Analysis of the European Union United States and China Experience and Implementation Prospects for CIS Countries

AIPCP25-CF-ICAIPSS2025-00436 | Article

Legal Regulation of Artificial Intelligence in the Energy Sector: A Comparative Analysis of the European Union, United States, and China Experience and Implementation Prospects for CIS Countries

Karligash Umarova[1,a)], Zukhra Reymova[2]

[1] *Karakalpak state university named after Berdakh, Nukus, Uzbekistan*
[2] *Law College of the Republic of Karakalpakstan, Nukus, Uzbekistan*

[a)] *Corresponding author: karligash1255@mail.ru*

Abstract. The accelerating integration of artificial intelligence technologies into critical energy infrastructure presents national legal systems with regulatory challenges requiring governance frameworks capable of addressing risks arising from autonomous decision-making while preserving opportunities for beneficial innovation. This study undertakes a comparative legal analysis of regulatory models governing AI applications in the energy sector across three major jurisdictions—the European Union, the United States, and the People's Republic of China—employing comparative legal, formal juridical, and systemic-structural methods to identify convergent principles and divergent approaches that may inform regulatory development in Commonwealth of Independent States countries. The analysis reveals four principal areas of international convergence: risk-based differentiation recognizing that AI applications in critical infrastructure warrant enhanced regulatory scrutiny; integration of AI governance with established cybersecurity frameworks; human oversight requirements for systems operating in safety-critical contexts; and incorporation of technical standards into regulatory architectures. Concurrently, significant divergences persist concerning the choice between comprehensive horizontal legislation and sector-specific approaches, the balance between mandatory requirements and voluntary mechanisms, and data governance regimes with varying emphases on localization and cross-border transfer restrictions. For CIS countries, the international experience supports adoption of risk-based classification frameworks, integration of AI governance with existing energy sector regulation, reference to international technical standards, and establishment of regulatory sandboxes for evidence-based policy development, while the common legal heritage and existing regional cooperation mechanisms create favorable conditions for coordinated approaches that may reduce regulatory development burdens and facilitate cross-border AI applications enhancing regional energy system efficiency.

INTRODUCTION

The accelerating deployment of artificial intelligence technologies across the energy sector presents national legal systems with regulatory challenges of unprecedented complexity and consequence. Machine learning algorithms increasingly permeate critical functions within electrical power systems—from demand forecasting and load optimization to predictive maintenance of grid infrastructure and real-time management of distributed energy resources—creating both substantial opportunities for enhanced system efficiency and significant risks arising from autonomous decision-making in sectors upon which modern economies fundamentally depend.

The urgency of systematic regulatory attention to this domain derives from several converging considerations. The energy sector constitutes critical infrastructure par excellence, the disruption of which carries potentially severe consequences for public safety, economic stability, and the provision of essential services to populations. Unlike conventional industrial equipment subject to established technical regulation regimes, artificial intelligence systems deployed in energy applications exhibit characteristics—including algorithmic opacity, emergent behaviors, and capacity for autonomous operation—that strain traditional regulatory paradigms premised on deterministic system behavior and comprehensive ex ante specification of operating parameters. Furthermore, the Commonwealth of Independent States find themselves at a formative stage in developing normative frameworks for artificial intelligence governance, rendering the systematic examination of international experience particularly salient for the elaboration of effective national approaches calibrated to specific institutional capacities and legal traditions.

The present study undertakes a comprehensive comparative legal analysis of regulatory models governing artificial intelligence applications in the energy sector across three major jurisdictions: the European Union, the United States of America, and the People's Republic of China. These jurisdictions have been selected not merely for their economic significance and technological advancement, but because they represent fundamentally distinct approaches to AI governance—comprehensive horizontal legislation supplemented by sectoral provisions in the European case, sector-specific mandatory standards combined with voluntary frameworks in the American tradition, and strategic state planning coupled with targeted regulation of specific AI modalities in the Chinese model. The examination of these divergent yet increasingly mature regulatory architectures provides an empirical foundation for identifying both convergent principles that may reflect emerging international consensus and divergent elements that offer alternative policy pathways for jurisdictions developing their own frameworks.

The methodological foundation of this research rests upon three complementary analytical approaches. The comparative legal method enables systematic identification of commonalities and distinctions across national regulatory frameworks, revealing both universal challenges inherent to AI governance in critical infrastructure and jurisdiction-specific responses shaped by particular legal traditions and institutional structures. Formal juridical analysis facilitates rigorous examination of legislative instruments, regulatory provisions, and technical standards that collectively constitute the normative architecture governing AI deployment in energy systems. The systemic-structural method ensures comprehensive consideration of the relationships between general AI regulation and sector-specific energy law provisions, recognizing that effective governance emerges from the interaction of multiple regulatory layers rather than from isolated interventions.

The scholarly contribution of this study lies in the systematic organization of dispersed normative sources across three leading jurisdictions into a coherent analytical framework, the identification of convergent and divergent elements in international approaches to a regulatory domain that remains in active development, and the formulation of adapted recommendations for CIS legal systems that account for their shared legal heritage, institutional capabilities, and energy market characteristics. As CIS countries navigate the complex task of establishing governance frameworks for AI applications in their power systems, the international experience documented herein offers both cautionary lessons and promising models that may inform the development of regulatory approaches suited to the specific circumstances of post-Soviet legal systems while maintaining compatibility with emerging international standards and facilitating beneficial technology transfer and regional cooperation.

REGULATORY MODELS FOR ARTIFICIAL INTELLIGENCE IN THE ENERGY SECTOR: THE EUROPEAN UNION AND UNITED STATES EXPERIENCE

The governance of artificial intelligence in the energy sector has emerged as a critical concern for jurisdictions worldwide, driven by the recognition that AI applications in power systems simultaneously offer substantial benefits and pose significant risks to critical infrastructure. As AI technologies become increasingly integral to grid operations, renewable energy integration, and energy market optimization, regulatory frameworks must evolve to address the unique challenges posed by autonomous decision-making systems in safety-critical environments. This section examines the principal international approaches to AI regulation in the energy sector, with particular attention to frameworks that offer insights applicable to CIS countries developing their own regulatory responses.

The international regulatory landscape exhibits considerable diversity in approaches to governing AI in critical infrastructure. Some jurisdictions have adopted comprehensive, horizontal AI legislation that applies across sectors, while others rely primarily on sector-specific technical standards and guidelines. The European Union has pioneered the most ambitious comprehensive framework through the AI Act, whereas the United States continues to employ a decentralized approach combining voluntary frameworks with sector-specific mandatory requirements. China has pursued a distinctive path emphasizing both strategic promotion of AI deployment and targeted regulation of specific applications [1]. Understanding these varied approaches provides essential context for CIS countries navigating the complex task of developing appropriate regulatory frameworks for their own energy sectors.

The European Union has established the world's first comprehensive legal framework for artificial intelligence through Regulation (EU) 2024/1689, commonly known as the AI Act. This landmark legislation entered into force on August 1, 2024, with full applicability scheduled for August 2, 2026, subject to certain transitional provisions [2]. The AI Act represents a fundamentally new approach to technology regulation, establishing harmonized rules for AI systems based on a risk-based classification methodology that differentiates regulatory requirements according to the potential impact of AI applications on safety and fundamental rights [3].

The risk-based approach categorizes AI systems into four tiers: unacceptable risk (prohibited), high-risk (subject to stringent requirements), limited risk (subject to transparency obligations), and minimal risk (largely unregulated). This tiered structure enables proportionate regulation that imposes substantial compliance burdens only where the potential for harm justifies such requirements [4]. The AI Act applies extraterritorially to providers and deployers outside the EU where the output produced by their AI systems is used within the Union [5], ensuring that foreign operators cannot circumvent regulatory requirements through jurisdictional arbitrage.

The AI Act's implications for the energy sector derive primarily from its classification of AI systems used in critical infrastructure as high-risk. Annex III of the Regulation specifically identifies "AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity" as high-risk applications [6]. This classification reflects the recognition that AI failures in energy systems could have severe consequences for public safety, economic stability, and essential services.

The designation of energy sector AI as high-risk encompasses a broad range of applications. AI systems controlling energy distribution networks, managing power flow optimization, conducting predictive maintenance of grid equipment, and operating automated protection systems all potentially fall within this classification [7]. Distributed Energy Resource Management Systems (DERMS) employing AI-driven algorithms to coordinate virtual power plants, microgrids, and smart grid operations are explicitly identified as requiring enhanced regulatory oversight [8]. Similarly, AI applications in energy trading and risk management that could impact market outcomes face strict governance requirements analogous to those in financial services.

Requirements for High-Risk AI Systems in Energy. Providers of high-risk AI systems in the energy sector must comply with comprehensive requirements spanning the entire AI lifecycle. These obligations include establishing robust risk management systems, ensuring high standards of data quality for training datasets, maintaining detailed technical documentation, implementing logging capabilities for traceability, providing clear instructions for deployers, enabling human oversight mechanisms, and ensuring appropriate levels of accuracy, robustness, and cybersecurity [9].

The conformity assessment requirements are particularly significant for energy sector applications. High-risk AI systems must undergo evaluation procedures before placement on the market or putting into service, with certain categories requiring third-party assessment by notified bodies. These procedures aim to verify that AI systems meet the essential requirements established by the Regulation and that providers have implemented appropriate quality management systems.

The human oversight requirements merit particular attention in the energy context. The AI Act mandates that high-risk systems be designed to enable effective oversight by natural persons during use, including the ability to understand system capabilities and limitations, monitor operations, interpret outputs, and intervene or interrupt system operation when necessary. For real-time grid operations where AI systems may make time-critical decisions, implementing meaningful human oversight while preserving the benefits of automated response presents significant technical and organizational challenges that energy sector regulators and operators must carefully navigate.

These challenges, however, do not arise in a regulatory vacuum. The AI Act operates within a broader EU framework for energy sector digitalization established primarily through the Clean Energy Package adopted in 2019. Directive (EU) 2019/944 on common rules for the internal market for electricity establishes foundational provisions for smart metering, data management, and consumer participation in electricity markets that create the technological substrate upon which AI applications operate [10]. In essence, the Clean Energy Package provides the digital infrastructure, while the AI Act governs how intelligent systems may be deployed within that infrastructure.

Central to this digital foundation is the deployment of smart metering systems. The Electricity Directive requires Member States to ensure that such systems assist active participation of customers in the electricity market, with at least 80 percent of final customers to be equipped with smart meters either within seven years of the date of the positive cost-benefit assessment or by 2024 for those Member States that had initiated systematic deployment before the Directive's entry into force [11]. These meters must satisfy minimum functional and technical standards ensuring interoperability with consumer energy management systems and smart grids. Beyond their immediate consumer benefits, these requirements establish the data infrastructure essential for AI-based demand forecasting, load management, and grid optimization applications—creating the informational ecosystem that AI systems require to function effectively.

Equally important are the data governance provisions that accompany smart meter deployment. The Directive addresses data management and access rights critical for AI applications, requiring that consumers and authorized third parties be able to access consumption data through standardized communication interfaces. This accessibility enables the data flows necessary for AI-based energy services while simultaneously imposing cybersecurity and data protection requirements to ensure consumer privacy. The resulting framework seeks to balance data-driven innovation with individual rights protection—a tension that becomes increasingly complex as AI systems process ever-larger volumes of consumer energy data.

Recognizing that regulatory frameworks must evolve alongside technological capabilities, the AI Act also establishes provisions for regulatory sandboxes—controlled environments where AI systems can be developed, tested, and validated under regulatory supervision before broader deployment [12]. For the energy sector specifically, these sandboxes offer valuable opportunities to evaluate innovative AI applications in grid management, renewable integration, and demand response while identifying regulatory obstacles and developing appropriate compliance approaches. Member States are required to establish at least one AI regulatory sandbox at national level, operational by August 2, 2026, with structured frameworks for testing that include appropriate safeguards for participants and affected persons. For energy applications, such sandboxes may enable grid operators and technology providers to assess AI systems under realistic conditions while maintaining necessary safety protections for critical infrastructure operations.

The European approach, characterized by comprehensive horizontal legislation supplemented by sector-specific provisions, stands in marked contrast to the regulatory philosophy prevailing in the United States. The United States has not adopted comprehensive federal AI legislation comparable to the EU AI Act; instead, AI governance in the energy sector relies on a combination of sector-specific mandatory standards, voluntary frameworks, and executive actions. This decentralized approach reflects the American regulatory tradition of addressing specific risks through targeted interventions rather than comprehensive ex-ante regulation, resulting in a more fragmented but potentially more adaptable governance landscape.

The institutional architecture of American energy regulation reinforces this fragmentation. The Federal Energy Regulatory Commission (FERC) exercises primary jurisdiction over interstate electricity transmission and wholesale electricity markets, while state public utility commissions regulate retail electricity services and local distribution. This divided regulatory structure means that AI applications in power systems may be subject to varying requirements depending on their specific functions and the aspects of the electricity system they affect—a complexity that providers of AI solutions must carefully navigate.

Within this decentralized framework, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards constitute the primary mandatory cybersecurity framework applicable to AI systems in the bulk electric system. These standards, enforceable through FERC authority, establish baseline security requirements for critical cyber assets that support reliable operation of the North American power grid. The NERC CIP framework encompasses thirteen core standards as of 2024, covering identification and categorization of cyber assets, security management controls, personnel security, electronic security perimeters, physical security, systems security management, incident reporting and response, recovery planning, configuration management, information protection, communications between control centers, and supply chain risk management [13]. AI systems operating within bulk electric system environments must comply with applicable CIP requirements based on their impact classification.

The evolving threat landscape has prompted continuous refinement of these standards. Recent developments in NERC CIP have enhanced requirements for internal network security monitoring, with FERC Order No. 887 directing NERC to develop standards requiring internal network security monitoring capabilities for high and medium impact bulk electric system cyber systems [14]. The proposed CIP-015 standard on Internal Network Security Monitoring reflects the growing sophistication of cyber threats to grid infrastructure and the need for enhanced visibility into network activities, including those involving AI systems. Nevertheless, it bears noting that the CIP standards were not specifically designed for AI applications, creating potential gaps in addressing AI-specific risks such as adversarial attacks on machine learning models, data poisoning, or algorithmic bias. The framework's requirements for configuration management, access controls, and security monitoring provide foundational protections applicable to AI-enabled systems, but the interplay between general cybersecurity requirements and AI-specific considerations represents an ongoing area of regulatory development.

Complementing these mandatory standards, the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), released in January 2023, provides voluntary guidance for managing risks associated with AI systems. While not legally binding, the AI RMF is increasingly recognized across public, private, and critical infrastructure sectors as a best-practice model for responsible AI risk management, with its principles referenced in government contracts, industry standards, and emerging state-level AI legislation. The framework establishes a flexible structure organized around four core functions: Govern, which addresses organizational context, culture, and accountability; Map, which focuses on identifying and assessing AI system characteristics and risks;

Measure, which involves analyzing and tracking AI risks and impacts; and Manage, which encompasses prioritizing and implementing risk responses [15]. The framework emphasizes trustworthiness characteristics including interpretability, validity, reliability, safety, security, resilience, accountability, transparency, explainability, privacy, and fairness.

For energy sector applications specifically, the AI RMF provides structured approaches to identifying and managing risks associated with AI systems in critical infrastructure. The framework's emphasis on context-specific risk assessment enables energy companies to tailor governance approaches to the particular requirements of grid operations, market participation, and customer service applications. While no formal mapping exists between the AI RMF and NERC CIP standards, the AI RMF's design allows energy companies to integrate its risk management principles with existing CIP compliance frameworks, leveraging prior NIST-NERC collaboration on Cybersecurity Framework mappings as a methodological model [16]. Building upon these foundational frameworks, the Department of Homeland Security in November 2024 released the "Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure," providing the first federal guidance specifically addressing AI governance in critical infrastructure sectors including energy. Developed in collaboration with industry leaders, the DHS Framework identifies specific stakeholders in the AI ecosystem—including AI developers, critical infrastructure owners and operators, and others—and assigns differentiated responsibilities to each category. AI developers are advised to test for biases, failure modes, and vulnerabilities, clearly identify AI-generated content, and support independent assessments for models presenting heightened risks to critical infrastructure [17]. Critical infrastructure owners and operators, meanwhile, are encouraged to implement strong cybersecurity practices for AI systems and provide meaningful transparency regarding AI use in services affecting the public. The Framework references the sixteen critical infrastructure sectors defined by the Cybersecurity and Infrastructure Security Agency (CISA), explicitly including the energy sector, and while voluntary, it provides actionable recommendations that energy companies can adopt to strengthen AI governance and prepare for potential future mandatory requirements.

The Department of Energy has similarly contributed to the emerging governance landscape through its Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which has developed guidance aligning energy sector practices with the NIST Cybersecurity Framework, including considerations for emerging technologies [18]. The Energy Sector Cybersecurity Framework Implementation Guidance provides energy companies with practical approaches to establishing cybersecurity programs consistent with federal frameworks. Beyond guidance documents, DOE has supported research and development initiatives exploring AI applications in grid modernization, including programs addressing cybersecurity challenges associated with AI-enabled grid technologies. These initiatives recognize both the potential benefits of AI for grid resilience and efficiency and the security implications of introducing autonomous decision-making systems into critical infrastructure, reflecting a pragmatic approach that seeks to enable innovation while managing attendant risks.

PEOPLE'S REPUBLIC OF CHINA: STRATEGIC PROMOTION AND TARGETED REGULATION

China has pursued a distinctive approach to AI governance that combines ambitious strategic promotion with targeted regulation of specific applications and sectors. Since 2013, the country has implemented successive national policies to facilitate AI development, including the Internet Plus Plan of Action and Made in China 2025 strategy. More recent initiatives, such as the Development Plan on Smart Manufacturing and the Overall Layout Plan for the Construction of Digital China, have further accelerated this trajectory. These foundational initiatives supported rapid expansion of AI applications across manufacturing, finance, education, logistics, and energy sectors, creating an environment conducive to technological innovation while establishing the groundwork for subsequent regulatory intervention.

Building upon this policy foundation, the New Generation Artificial Intelligence Development Plan issued in 2017 elevated AI to a matter of national strategic priority, establishing comprehensive objectives for AI development and establishing comprehensive objectives for AI development that laid groundwork for subsequent sector-specific applications, including in the energy domain. This strategic framework positioned AI as central to economic modernization and technological competitiveness, with explicit attention to energy system optimization as a driver of both industrial efficiency and national security.

The strategic vision articulated in these earlier policies culminated in sector-specific implementation guidance when, in September 2025, the National Development and Reform Commission (NDRC) and National Energy Administration (NEA) jointly issued the "Implementation Opinions on Promoting High-Quality Development of

‘AI+’ Energy”. This document represents the most detailed national policy framework specifically addressing AI in energy systems among major jurisdictions, translating broad strategic objectives into concrete development priorities. The Implementation Opinions establish phased objectives reflecting China’s characteristic approach of setting measurable targets within defined timeframes: by 2027, the country aims to establish foundational innovation systems for AI-energy integration and launch demonstration projects across key scenarios; by 2030, the goal is global leadership in AI-energy integration, supported by advanced platforms and comprehensive policy frameworks [19]. These milestones position AI as a strategic enabler of national energy security, with applications spanning predictive maintenance, intelligent dispatching, and autonomous operations.

The scope of applications identified in the plan demonstrates the comprehensive nature of China’s approach. Specific domains include AI-enhanced grid security and renewable energy integration through improved forecasting and automated planning; AI applications in virtual power plants, electric vehicle-grid interaction, and carbon trading; intelligent operations and maintenance for hydropower, thermal power, and nuclear facilities; and autonomous mining and hazard detection in coal operations. This comprehensive coverage reflects China’s strategy of leveraging AI across the entire energy value chain while maintaining centralized coordination of development priorities—an approach that contrasts with the more decentralized, market-driven development characteristic of Western jurisdictions.

While these sector-specific policies provide direction for AI deployment in energy systems, China’s general AI regulatory framework establishes the broader governance context within which such applications operate [20]. The regulatory architecture has evolved through a series of technology-specific interventions addressing particular AI modalities and functionalities. The earliest of these targeted regulations, the Internet Information Service Algorithmic Recommendation Management Provisions, took effect in March 2022, followed by the Internet Information Service Deep Synthesis Management Provisions in January 2023. These measures address specific AI functionalities with emphasis on security, content control, and alignment with national values—regulatory priorities that differ markedly from the rights-based approach characteristic of EU regulation. The Interim Measures for the Management of Generative Artificial Intelligence Services, effective August 15, 2023, extended this approach to generative AI, establishing the first administrative regulation specifically governing such services [21]. While focused primarily on content generation rather than industrial applications, these measures illustrate China’s consistent methodology of targeted intervention addressing specific AI modalities as they emerge and mature.

Complementing this regulatory framework, the national standards system provides technical requirements that translate regulatory mandates into practical compliance guidance. The Technical Committee 260 (TC260) has released standards including Basic Security Requirements for Generative Artificial Intelligence Services, offering concrete specifications for AI system security. For energy sector AI applications, the combination of sector-specific policy direction from NDRC and NEA with general AI standards from TC260 creates a multi-layered governance structure that addresses both industrial development objectives and security concerns.

A particularly significant aspect of this governance architecture with direct implications for the energy sector concerns data localization and cross-border transfer restrictions. The Data Security Law and Cybersecurity Law establish the legal foundation for data governance, including stringent requirements for critical information infrastructure operators - a category that encompasses major energy facilities [22]. Under these frameworks, AI applications in energy systems must store data within China and face substantial restrictions on cross-border transfers. These requirements reflect broader data sovereignty concerns and have significant implications for international technology providers seeking to deploy AI solutions in Chinese energy markets, creating compliance challenges that favor domestic technology development and may limit foreign vendor participation in sensitive grid applications.

Beyond domestic regulation, China has increasingly engaged in international AI governance discussions, seeking to shape emerging global frameworks. The Global AI Governance Initiative announced in 2023 and the subsequent Action Plan for Global Artificial Intelligence Governance released in July 2025 propose international frameworks for AI cooperation. These initiatives emphasize infrastructure development, technology transfer to developing countries, and establishment of common standards—priorities that reflect China’s position as both a major AI developer and a proponent of alternative governance models to those advanced by Western nations. For the energy sector specifically, China’s international engagement includes proposals for unified computing power standards and standards for AI-related energy efficiency—matters of direct relevance to data center energy consumption and grid integration challenges facing all major economies. The proposed establishment of a global AI cooperation organization, potentially headquartered in Shanghai, would provide institutional mechanisms for coordinating AI governance across jurisdictions, including in critical infrastructure sectors. Whether such proposals gain international traction remains to be seen, but they signal China’s ambition to influence not only domestic but also global approaches to AI governance in energy and other strategic sectors.

COMPARATIVE ANALYSIS AND IMPLICATIONS FOR CIS COUNTRIES

The preceding examination of regulatory approaches across major jurisdictions reveals both convergent principles and significant divergences that merit systematic analysis. While the European Union, United States, and China have developed distinct governance architectures reflecting their respective legal traditions, institutional structures, and policy priorities, certain foundational elements demonstrate remarkable consistency across these disparate frameworks—suggesting the emergence of international consensus on core principles applicable to AI governance in critical infrastructure sectors.

Perhaps the most fundamental point of convergence concerns the principle of risk-based differentiation. All major frameworks recognize that AI applications deployed within critical infrastructure warrant enhanced regulatory scrutiny compared to applications presenting lower risk profiles. This principle manifests differently across jurisdictions: the EU AI Act explicitly classifies energy sector AI systems as high-risk applications subject to mandatory conformity assessment procedures; the NERC CIP framework employs impact-based categorization that scales cybersecurity requirements according to the potential consequences of system compromise; and China's sector-specific policies direct heightened attention to energy applications through dedicated implementation guidance issued by specialized regulatory authorities. Despite these methodological variations, the underlying recognition that context-specific risk assessment should inform regulatory intensity represents a shared analytical foundation.

Closely related to this risk-based orientation is the consistent emphasis on cybersecurity integration across all examined frameworks [23]. The introduction of AI systems into energy infrastructure creates novel attack surfaces and vulnerabilities that existing cybersecurity frameworks were not designed to address, yet jurisdictions have generally chosen to extend and adapt established cybersecurity requirements rather than create entirely separate governance structures. The NERC CIP standards provide mandatory cybersecurity requirements that increasingly encompass AI-enabled systems; EU requirements for high-risk AI systems incorporate security considerations alongside safety and fundamental rights protections; and Chinese data security regulations establish stringent requirements for critical information infrastructure operators that directly affect AI deployment in energy systems. This integration reflects practical recognition that AI security cannot be meaningfully addressed in isolation from broader infrastructure cybersecurity.

A third convergent element concerns human oversight requirements for AI systems operating in safety-critical contexts [24]. International frameworks consistently emphasize that autonomous AI decisions affecting critical infrastructure should remain subject to human review and intervention capabilities, though the specific mechanisms prescribed for ensuring such oversight vary considerably [25]. This principle reflects both technical prudence—acknowledging current limitations in AI system reliability and explainability—and normative commitments to maintaining human accountability for consequential infrastructure decisions. The practical implementation of human oversight requirements presents ongoing challenges as AI systems assume increasingly autonomous operational roles, but the principle itself enjoys broad international endorsement.

The integration of technical standards into regulatory frameworks represents a fourth area of convergence with significant practical implications. Rather than specifying detailed technical requirements within legislation or regulations, jurisdictions increasingly reference or incorporate standards developed through specialized technical bodies. This approach enables detailed specification of implementation requirements while preserving flexibility to adapt to technological evolution through standards development processes that operate more dynamically than formal legislative procedures. The relationship between mandatory regulations and voluntary standards varies across jurisdictions, but the general tendency toward standards integration reflects recognition that effective AI governance requires technical specificity that regulatory instruments alone cannot efficiently provide.

Notwithstanding these convergent elements, significant divergences in international approaches warrant careful consideration by policymakers developing governance frameworks for new jurisdictions. The most fundamental divergence concerns the choice between comprehensive horizontal legislation and sector-specific regulatory approaches. The European Union has adopted comprehensive AI legislation applicable across all sectors, establishing uniform requirements that apply regardless of the specific domain of AI deployment while permitting sector-specific supplementation. The United States, by contrast, relies primarily on sector-specific mandatory requirements—such as the NERC CIP standards for bulk electric systems—supplemented by voluntary frameworks like the NIST AI RMF that provide guidance without imposing legal obligations. China combines elements of both approaches, with national strategic planning documents establishing overarching policy direction while targeted regulations address specific AI modalities such as algorithmic recommendation systems, deep synthesis technologies, and generative AI services.

Each approach presents distinct advantages and limitations that reflect underlying differences in legal systems, institutional capacities, and policy philosophies.

The balance between mandatory requirements and voluntary mechanisms constitutes a related but distinct dimension of regulatory divergence. EU requirements for high-risk AI systems are mandatory, with substantial penalties for non-compliance that may reach significant percentages of global annual turnover. This approach prioritizes regulatory certainty and enforcement capability but may impose compliance burdens that affect innovation trajectories. U.S. frameworks like the NIST AI RMF remain formally voluntary, though their practical significance increases as they become referenced in government procurement requirements and private contractual arrangements. Chinese approaches employ both mandatory regulations—particularly for AI services with public opinion attributes or social mobilization capabilities—and non-binding standards that guide implementation without creating legal obligations. The appropriate balance between mandatory and voluntary mechanisms depends substantially on institutional enforcement capabilities, market structures, and policy objectives that vary across jurisdictions.

Data governance approaches associated with AI systems present perhaps the most pronounced divergence among major jurisdictions. China emphasizes data localization and sovereignty, requiring that data generated by critical information infrastructure operators be stored within national territory and subjecting cross-border transfers to security assessments and regulatory approval. These requirements have significant implications for international technology providers and reflect broader policy objectives concerning data sovereignty and national security. The European Union applies comprehensive data protection requirements through the General Data Protection Regulation alongside sector-specific provisions, creating an integrated framework that addresses both personal data and critical infrastructure data governance. United States approaches remain more fragmented, with data governance addressed through various sector-specific frameworks, state-level legislation, and voluntary industry practices rather than comprehensive federal legislation. These divergent approaches to data governance create compliance challenges for technology providers operating across multiple jurisdictions and influence the practical feasibility of international AI deployment in energy sectors.

The international experience documented in preceding sections offers several substantive lessons for CIS countries developing regulatory frameworks for AI applications in power supply systems. The principle of risk-based classification provides a pragmatic foundation that enables proportionate regulatory requirements without impeding beneficial innovation. CIS countries may productively consider frameworks that identify energy sector AI as warranting enhanced oversight—reflecting the critical infrastructure status of power systems—while preserving regulatory flexibility for lower-risk applications that do not directly affect grid stability or safety. Such approaches align with emerging international consensus while permitting adaptation to specific national circumstances and institutional capabilities.

Integration of AI governance with existing energy sector regulation and cybersecurity frameworks offers significant advantages over the creation of entirely separate regulatory structures. CIS countries possess established electricity sector regulatory frameworks and increasingly developed cybersecurity requirements that provide institutional foundations for AI governance [26]. Building on these existing structures promotes regulatory coherence, leverages accumulated institutional expertise, and reduces the risk of creating conflicting or duplicative requirements. The practical implementation of AI governance through existing regulatory channels may prove more effective than establishing new specialized agencies or frameworks that lack established relationships with regulated entities and operational experience in the energy sector [27].

International standards offer mechanisms for harmonization that can reduce compliance burdens for technology providers while ensuring adequate protections for critical infrastructure. CIS countries may reference international standards—including those developed through organizations such as ISO, IEC, and ITU—as technical foundations for national requirements while adapting governance approaches to reflect specific national circumstances, legal traditions, and policy priorities. This approach facilitates technology transfer and international cooperation while preserving regulatory sovereignty. The ongoing development of AI-specific international standards presents opportunities for CIS countries to participate in standards-setting processes and ensure that emerging international frameworks reflect their interests and circumstances.

Regional cooperation mechanisms within the CIS framework provide established channels for information sharing, capacity building, and regulatory harmonization that may be productively leveraged for AI governance in the energy sector. The common legal heritage of CIS countries, shared experience with energy sector regulation, and existing institutional mechanisms for cooperation create favorable conditions for coordinated approaches to AI governance. Such coordination can reduce duplication of regulatory development efforts, facilitate cross-border AI applications that enhance regional energy system efficiency, and strengthen collective capacity to address the governance challenges presented by rapidly evolving AI technologies [28].

Finally, regulatory sandboxes and pilot projects offer mechanisms for evidence-based policy development that may prove particularly valuable given the novelty of AI applications in energy systems and the limited empirical basis for regulatory design. CIS countries may establish controlled environments for testing innovative AI solutions that enable practical experience to inform regulatory development. Such approaches allow regulators to observe AI system performance under realistic conditions, identify unforeseen risks or benefits, and develop regulatory requirements grounded in empirical evidence rather than theoretical assumptions. The EU AI Act's provisions for regulatory sandboxes and China's emphasis on demonstration projects provide models that CIS countries may adapt to their specific circumstances while developing permanent regulatory frameworks suited to their energy sectors and institutional contexts.

CONCLUSIONS

The comparative legal analysis undertaken in this study reveals that the governance of artificial intelligence applications in the energy sector, while still in formative stages across all examined jurisdictions, has begun to coalesce around certain foundational principles even as significant divergences persist in regulatory methodology and institutional architecture. The European Union, United States, and People's Republic of China have each developed distinctive approaches that reflect their respective legal traditions, institutional capacities, and policy priorities—yet the examination of these varied frameworks discloses convergent elements that may constitute an emerging international consensus on core principles applicable to AI governance in critical infrastructure sectors.

The analysis identifies four principal areas of convergence across the examined jurisdictions. First, the principle of risk-based differentiation enjoys universal recognition, with all major frameworks acknowledging that AI applications deployed within critical energy infrastructure warrant enhanced regulatory scrutiny commensurate with their potential consequences for public safety, economic stability, and essential services. Second, the integration of AI governance with established cybersecurity frameworks reflects practical recognition that the novel vulnerabilities introduced by intelligent systems cannot be meaningfully addressed in isolation from broader infrastructure protection requirements. Third, human oversight requirements for AI systems operating in safety-critical contexts receive consistent emphasis across jurisdictions, reflecting both technical prudence regarding current limitations in AI reliability and normative commitments to maintaining human accountability for consequential infrastructure decisions. Fourth, the incorporation of technical standards into regulatory architectures enables detailed specification of implementation requirements while preserving flexibility to accommodate technological evolution through standards development processes that operate more dynamically than formal legislative procedures.

Notwithstanding these convergent elements, the analysis documents significant divergences that present alternative pathways for jurisdictions developing their own regulatory frameworks. The choice between comprehensive horizontal legislation—as exemplified by the EU AI Act—and sector-specific regulatory approaches characteristic of the United States represents a fundamental architectural decision with substantial implications for regulatory coherence, compliance burdens, and adaptability to technological change. The balance between mandatory requirements and voluntary mechanisms varies considerably across jurisdictions, reflecting different assessments of institutional enforcement capabilities, market structures, and the appropriate relationship between regulatory prescription and industry self-governance. Data governance approaches present perhaps the most pronounced divergence, with Chinese data localization requirements, European comprehensive data protection frameworks, and fragmented American approaches creating distinct compliance landscapes for technology providers and influencing the practical feasibility of international AI deployment in energy sectors.

For the Commonwealth of Independent States, the international experience documented herein offers several substantive lessons that may inform the development of regulatory frameworks calibrated to the specific circumstances of post-Soviet legal systems. The principle of risk-based classification provides a pragmatic foundation that enables proportionate regulatory requirements without impeding beneficial innovation, and CIS countries may productively consider frameworks that identify energy sector AI as warranting enhanced oversight while preserving regulatory flexibility for lower-risk applications. Integration of AI governance with existing energy sector regulation and cybersecurity frameworks offers significant advantages over the creation of entirely separate regulatory structures, leveraging accumulated institutional expertise and established relationships with regulated entities. Reference to international standards can reduce compliance burdens while ensuring adequate protections, and participation in standards-setting processes presents opportunities for CIS countries to ensure that emerging international frameworks reflect their interests and circumstances.

The common legal heritage of CIS countries, shared experience with energy sector regulation, and existing institutional mechanisms for regional cooperation create favorable conditions for coordinated approaches to AI governance that may reduce duplication of regulatory development efforts, facilitate cross-border AI applications enhancing regional energy system efficiency, and strengthen collective capacity to address governance challenges presented by rapidly evolving technologies. Regulatory sandboxes and pilot projects offer mechanisms for evidence-based policy development particularly valuable given the novelty of AI applications in energy systems and the limited empirical foundation currently available for regulatory design.

The limitations of the present study suggest directions for future research. The analysis has necessarily focused on formal regulatory frameworks and policy documents, with limited attention to implementation experience and enforcement practices that remain nascent given the recent adoption of many examined provisions. As jurisdictions accumulate practical experience with AI governance in energy systems, empirical studies examining regulatory effectiveness, compliance costs, and innovation impacts will provide essential evidence for refining governance approaches. Additionally, the development of model legislative instruments specifically adapted to CIS legal traditions and institutional contexts would facilitate harmonized regional approaches while reducing the burden on individual jurisdictions to develop frameworks independently. Finally, the rapid evolution of AI technologies—including the emergence of increasingly autonomous systems and novel application domains—will require ongoing attention to ensure that regulatory frameworks remain adequate to address risks that may not be fully anticipated by current provisions.

The governance of artificial intelligence in critical energy infrastructure represents a regulatory challenge of considerable complexity, requiring careful calibration of protective requirements with innovation objectives, harmonization of general AI governance with sector-specific energy regulation, and coordination across jurisdictions operating within an increasingly interconnected global energy system. The international experience examined in this study demonstrates that while no single regulatory model offers a universally applicable template, the systematic analysis of diverse approaches provides valuable insights for jurisdictions navigating the complex task of developing governance frameworks suited to their particular circumstances. For CIS countries, the opportunity exists to draw upon this international experience while crafting regulatory responses that reflect their shared legal heritage, institutional capabilities, and energy sector characteristics—contributing to the emerging global dialogue on AI governance while ensuring that the benefits of intelligent systems in energy applications can be realized without compromising the safety, security, and reliability of critical infrastructure upon which their populations depend.

REFERENCES

1. C. Yang, C. Huang. Quantitative mapping of the evolution of AI policy distribution, targets and focuses over three decades in China. Technological Forecasting and Social Change (2022) 174: 121188. https://doi.org/10.1016/j.techfore.2021.121188
2. European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). Official Journal of the European Union (2024) L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
3. Z. A. Ashraf, N. Mustafa. AI standards and regulations. Intersection of Human Rights and AI in Healthcare (2025): 325-352. https://doi.org/10.4018/979-8-3693-7051-3.ch014
4. European Parliament. EU AI Act: first regulation on artificial intelligence. Topics (2024) Article 20230601STO93804.
5. M. Czerniawski. Towards the Effective Extraterritorial Enforcement of the AI Act. In: J. H. Hoepman, M. Jensen, M. G. Porcedda, S. Schiffner, S. Ziegler (eds) Privacy Symposium 2024. DPLICIT 2024. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-76265-9_3
6. M. Mueck, C. Gaie, D. C. Gkikas. Introduction to the European Artificial Intelligence Act. In: M. Mueck, C. Gaie (eds) European Digital Regulations. Intelligent Systems Reference Library (2025) vol. 265. Springer, Cham. https://doi.org/10.1007/978-3-031-80809-8_3
7. P. Arévalo, F. Jurado. Impact of artificial intelligence on the planning and operation of distributed energy systems in smart grids. Energies (2024) 17(17): 4501. https://doi.org/10.3390/en17174501
8. G. Rajendran, R. Raute, C. Caruana. The Brain Behind the Grid: A Comprehensive Review on Advanced Control Strategies for Smart Energy Management Systems. Energies (2025) 18(15): 3963. https://doi.org/10.3390/en18153963

9. T. Minssen, B. Solaiman, L. Köttering, J. Wested, A. Malik. Governing AI in the European Union: emerging infrastructures and regulatory ecosystems in health. Research Handbook on Health, AI and the Law (2024): 311-331. https://doi.org/10.4337/9781802205657.ch18
10. European Parliament and Council. Directive (EU) 2019/944 on common rules for the internal market for electricity. Official Journal of the European Union (2019) L 158. https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=oj:JOL_2019_158_R_0004
11. A. Clifton, S. Barber, A. Bray, P. Enevoldsen, J. Fields, A. M. Sempreviva, Y. Ding. Grand challenges in the digitalisation of wind energy. Wind Energy Science (2023) 8(6): 947-974. https://doi.org/10.5194/wes-8-947-2023
12. J. Truby, R. D. Brown, I. A. Ibrahim, O. C. Parellada. A sandbox approach to regulating high-risk artificial intelligence applications. European Journal of Risk Regulation (2022) 13(2): 270-294. https://doi.org/10.1017/err.2021.52
13.
14. Y. Benghename, A. Lounis, M. Sallak, W. Schön. Cybersecurity Standards Across Industries: A Critical Analysis of Current Practices and Future Directions in the Railway Sector. IEEE Transactions on Intelligent Transportation Systems (2025) 26(12): 21371-21392. https://doi.org/10.1109/TITS.2025.3615531
15. NIST AI Resource Center. AI RMF Core Functions (2023). https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF
16. C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, J. Johnson. Cyber security primer for DER vendors, aggregators, and grid operators. Technical Report (2017): 12.
17. M. I. Faruk, F. W. Plabon, U. S. Saha, M. D. Hossain. AI-Driven Project Risk Management: Leveraging Artificial Intelligence to Predict, Mitigate, and Manage Project Risks in Critical Infrastructure and National Security Projects. Journal of Computer Science and Technology Studies (2025) 7(6): 123-137. https://doi.org/10.32996/jcsts.2025.7.6.16
18. R. E. Reyes-Acosta, R. Mendoza-González, E. Oswaldo Diaz, M. Vargas Martin, F. J. Luna Rosas, J. C. Martínez Romo, A. Mendoza-González. Cybersecurity Conceptual Framework Applied to Edge Computing and Internet of Things Environments. Electronics (2025) 14(11): 2109. https://doi.org/10.3390/electronics14112109
19. P. D. E. Mutambara. Strategic Framework for AI Deployment. In: Deploying Artificial Intelligence to Achieve the UN Sustainable Development Goals. Sustainable Development Goals Series. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-88423-8_11
20. F. Heymann, K. Parginos, A. Hariri, G. Franco. Regulating artificial intelligence in the EU, United States and China — Implications for energy systems. In: 2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE) (2023): 1-6. IEEE. https://hal.science/hal-04167091/document
21. X. Wang, Y. C. Wu. Balancing innovation and regulation in the age of generative artificial intelligence. Journal of Information Policy (2024) 14: 385-416. https://doi.org/10.5325/jinfopoli.14.2024.0012
22. E. Mugamba. Global Data Governance in Digital Law: A Comparative Analysis of EU and Global Approaches to Cybersecurity Legislation. Journal of Smart Computing and Quantum Technologies (2025) 1(1): 1-19.
23. J. Boehm, N. Curcio, P. Merrath, L. Shenton, T. Stähle. The risk-based approach to cybersecurity. McKinsey, New York (2019). https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights
24. J. Perez-Cerrolaza, J. Abella, M. Borg, C. Donzella, J. Cerquides, F. J. Cazorla, J. L. Flores. Artificial intelligence for safety-critical systems in industrial and transportation domains: A survey. ACM Computing Surveys (2024) 56(7): 1-40. https://doi.org/10.1145/3626314
25. J. Panabergenova. Fulfilling fiduciary duties in the AI era: emerging risks and responsibilities in AI-assisted corporate financial oversight. Society and Innovations (2024) 5(2/S): 222–230. https://doi.org/10.47689/2181-1415-vol5-iss2/S-pp222-230
26. J. Panabergenova, K. Umarova. Corporate governance cybersecurity framework in CIS countries: comparative analysis of regulatory standards and digital risk management practices. International Cybersecurity Law Review (2025) 6: 367–376. https://doi.org/10.1365/s43439-025-00146-4
27. B. N. Jørgensen, Z. G. Ma. Regulating AI in the Energy Sector: A Scoping Review of EU Laws, Challenges, and Global Perspectives. Energies (2025) 18(9): 2359. https://doi.org/10.3390/en18092359
28. P. Jamilya, U. Karligash. Legal Challenges of Using Artificial Intelligence in Corporate Governance in Post-Soviet Countries. In: X. S. Yang, S. Sherratt, N. Dey, A. Joshi (eds) Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024. Lecture Notes in Networks and Systems (2024) vol. 1004. Springer, Singapore. https://doi.org/10.1007/978-981-97-3305-7_31