## KAPITEL 2 / *CHAPTER 2* [2]
## EU REGULATIONS IN AI IN THE ENERGY SECTOR: A Review

**DOI: 10.30890/2709-2313.2025-40-02-002**

The rapid digitalization of the energy sector is increasingly powered by artificial intelligence (AI), enabling advances in smart grid management, predictive maintenance, market forecasting, and demand response. However, integrating AI into critical energy infrastructure also raises complex regulatory challenges, particularly around cybersecurity, data privacy, market integrity, and safety.

The European Union (EU) has responded with a comprehensive regulatory framework, including the Artificial Intelligence Act (AI Act), GDPR, NIS2 Directive, Cyber Resilience Act (CRA), Network Code on Cybersecurity (NCCS), and the EU Cybersecurity Act. These laws impose strict compliance requirements for high-risk AI applications such as grid operations and market automation. While they enhance accountability and public trust, they also introduce legal complexities, potential innovation bottlenecks, and increased compliance costs.

Despite these challenges, AI offers transformative potential—machine learning models can optimize power dispatch or forecast renewable generation in real time. Yet, due to the energy sector's critical role, unregulated AI use can pose significant risks, including grid instability or privacy violations. Thus, a robust legal framework is essential to balance innovation with public interest protections.

The goal is to guide policymakers and stakeholders in aligning AI innovation with legal safeguards, ensuring energy sector resilience, security, and progress. Specifically, this review:

1. Summarizes key EU regulations affecting AI in energy,
2. Analyzes their impact on AI development and deployment across the energy value chain,
3. Compares the EU's regulatory stance with that of the U.S. and China, and
4. Identifies challenges and offers recommendations for harmonizing AI

[2]***Authors:*** *Mysak Ihor Vasylovych, Mysak Pavlo Vasylovych*
***Number of characters:*** *23987*
***Author's sheets:*** *0,60*

governance.

## 2.1. EU regulations in the AI area

In this section we summarized the main EU legal instruments regulating AI-driven digital solutions in the energy sector. It covers both AI-specific legislation, such as the proposed Artificial Intelligence Act (AI Act), and broader frameworks addressing cybersecurity and data protection. Key regulations include the AI Act, GDPR, NIS2 Directive, Cyber Resilience Act (CRA), Network Code on Cybersecurity (NCCS), and the EU Cybersecurity Act. Each is reviewed for its relevance to AI development, deployment, and operation in energy applications. A summary matrix at the end of this section outlines their applicability across different energy domains. The AI Act, proposed in 2021 and expected to be adopted by 2025, is the EU's first comprehensive regulation for AI. It introduces a risk-based classification system:

- **Prohibited AI**: Bans certain harmful uses, such as social scoring or manipulative AI—generally not relevant to energy.
- **High-risk AI**: Covers systems used in critical infrastructure, including energy. For example, AI tools managing grid operations or power generation fall under this category. These systems must meet strict requirements on risk management, data quality, transparency, technical documentation, and conformity assessment.
- **Limited-risk AI**: Requires transparency measures, such as AI self-identification in customer service applications.
- **Minimal-risk AI**: Low-risk tools, like internal analytics, are largely exempt from regulation but encouraged to follow voluntary standards.

For the energy sector, the AI Act introduces the first targeted compliance regime. Energy companies must determine whether their AI systems are classified as high-risk—likely if they impact safety or reliability—and comply with obligations such as human oversight and registration in an EU database. While the Act aims to balance innovation with safeguards for rights and public safety, some risks (e.g., market manipulation or cybersecurity) may not be fully addressed. In force since May 2018,

the GDPR is the EU's core data protection law, shaping how AI systems in the energy sector—especially on the demand side—handle personal data. It governs the use of smart meter data, consumption profiles, billing records, and personalized energy services.

Key implications for AI in energy include:

- **Legal basis and purpose limitation**: AI systems processing personal data must have a lawful basis such as consent or contractual necessity and cannot repurpose data for unrelated uses without new consent.
- **Data minimization and privacy by design**: Companies must limit data collection to what is necessary and embed privacy into system design. Anonymization and aggregation are encouraged to avoid using personally identifiable information.
- **Automated decision-making**: Individuals have rights when AI makes impactful decisions. Providers must ensure human oversight and offer explanations when such profiling occurs.
- **Security and breach notification**: Personal data must be protected from breaches, with mandatory reporting to authorities within 72 hours. Securing AI training data and systems is essential.
- **Data Protection Impact Assessments (DPIAs)**: Required when AI poses high privacy risks—common in smart home or city applications. DPIAs help identify and mitigate privacy threats.

While GDPR compliance can be seen as a regulatory hurdle—particularly for data-hungry AI models—it also builds consumer trust. It encourages privacy-conscious design, responsible data governance, and contractual safeguards with vendors. Importantly, GDPR remains fully applicable alongside the AI Act. High-risk AI systems must therefore meet both safety and privacy requirements, making dual compliance a central concern for AI innovation in the energy sector.

The Directive on the Security of Network and Information Systems (NIS2) represents the cornerstone of the European Union's cybersecurity framework for critical infrastructure. Adopted in 2022 as a successor to the original NIS Directive of

2016, NIS2 significantly elevates the EU's cybersecurity posture by harmonizing security standards across Member States and expanding the directive's applicability to a broader array of essential sectors, including energy. The energy domain—encompassing electricity, gas, oil, and district heating—is explicitly designated within the scope of NIS2 [2], thereby subjecting a wide range of organizations within the sector to enhanced cybersecurity obligations. While NIS2 is not explicitly focused on artificial intelligence (AI), its implications for AI systems in the energy sector are both substantial and indirect, as the directive imposes overarching digital security requirements that necessarily encompass AI-enabled solutions.

Under the NIS2 framework, medium and large-scale organizations operating within the energy sector are designated as "essential entities" and must therefore comply with the directive's mandates. NIS2 obliges covered entities to adopt "appropriate and proportionate" risk management practices spanning technical, operational, and organizational domains. These requirements encompass activities such as risk assessments, vulnerability management, business continuity planning, incident detection and response, and secure software development. For AI systems embedded within operational technologies (OT), these mandates translate into concrete security expectations. For example, an AI system responsible for voltage regulation in a smart grid must be developed and maintained using secure coding practices, be subject to regular penetration testing, and be protected against adversarial threats and data poisoning attacks. AI pipelines must also ensure secure data handling and model integrity, with safeguards against manipulation, model inversion, and inference attacks. The directive explicitly calls for adoption of "state-of-the-art" cybersecurity practices [3], raising the bar for AI systems that may historically have been deployed without rigorous security oversight.

A notable feature of NIS2 is its strict incident notification regime, which requires essential entities to report significant cybersecurity incidents to national competent authorities—such as Computer Security Incident Response Teams (CSIRTs)—typically within 24 hours of detection [1]. If an AI-driven energy management system is compromised—through unauthorized access, adversarial manipulation, or functional

disruption—such an incident must be promptly reported. This underscores the importance of continuous monitoring of AI behavior to detect anomalies or performance deviations that could indicate compromise. Furthermore, the upcoming Network Code on Cybersecurity for electricity, which aligns closely with NIS2, extends these reporting requirements with sector-specific protocols [5], thereby ensuring coherence in incident response across the energy landscape.

NIS2 places a strong emphasis on supply chain resilience, mandating that essential entities assess and manage cybersecurity risks associated with third-party suppliers and digital service providers [1]. In practice, this means that AI software, cloud infrastructure, and external analytics tools used by energy companies must be scrutinized for security posture. Entities are expected to maintain documentation detailing how cybersecurity risks are identified, managed, and mitigated—including for AI components. Supervisory authorities retain the right to audit compliance and impose corrective actions or penalties for deficiencies. As a result, the directive promotes the use of certified AI tools, vetted vendors, and well-documented development and deployment practices.

NIS2 also mandates that each Member State develop a comprehensive national cybersecurity strategy that encompasses critical sectors such as energy [4]. This strategic alignment creates an enabling environment for energy organizations to seek technical support, share best practices, and engage in collaborative initiatives to secure AI systems. Notably, the EU Cyber Crisis Liaison Organization Network (EU-CyCLONe) is tasked with managing large-scale cyber incidents, including those triggered by or affecting AI-based infrastructure [5]. In the event of a systemic AI-driven disruption—such as a coordinated cyberattack on grid automation tools—Member States can rely on this coordinated framework to mount an effective response.

The Cyber Resilience Act (CRA), adopted in 2024, represents a significant regulatory milestone in the European Union's approach to digital security. It establishes binding cybersecurity requirements for a broad range of digital products—both hardware and software—throughout their lifecycle. In contrast to the NIS2 Directive, which focuses on cybersecurity governance at the organizational level, the

CRA targets the inherent security of digital products themselves. This dual-pronged regulatory approach is particularly pertinent for the energy sector, where digitalization is rapidly advancing through the deployment of connected devices, industrial control systems, and AI-enabled software.

The CRA's implications for the energy sector are substantial, as modern energy infrastructure increasingly relies on digital components such as IoT sensors, control systems, edge computing platforms, and software applications that often embed artificial intelligence (AI). Although the regulation does not single out AI, its requirements apply fully to AI systems categorized as digital products. As such, developers, vendors, and energy organizations must ensure that their digital products—including AI-driven solutions—adhere to the CRA's robust security standards. The CRA encompasses virtually all hardware and software products with a digital component, with limited exceptions for items already regulated under other EU frameworks (e.g., medical devices) [6]. This includes general-purpose software, embedded systems, connected consumer devices, and enterprise solutions. In the context of the energy sector, this broad scope captures products such as smart meters, electric vehicle (EV) charging stations, advanced grid control equipment, supervisory control and data acquisition (SCADA) systems, and home energy management platforms. Even specialized AI software libraries or cloud-hosted analytics engines integrated into these systems fall within the CRA's regulatory reach.

Manufacturers and software developers are required to ensure that their digital products meet a series of baseline cybersecurity criteria. These include protection against unauthorized access, the implementation of secure-by-design and secure-by-default principles, maintenance of data confidentiality and integrity, and the timely mitigation of known vulnerabilities [7]. The CRA mandates that security be embedded from the earliest design stages and maintained throughout the product's lifecycle, including through the release of timely updates and patches. For instance, AI software managing wind turbine operations must avoid insecure configurations such as hardcoded credentials and must have a documented vulnerability management protocol. Failure to meet these standards not only poses operational risks but may also

render the product non-compliant with EU market requirements.

The CRA entered into force in 2024, with a structured implementation phase culminating in full application of its obligations from 2027 onward [10]. This grace period provides a finite window for manufacturers, AI startups, and energy utilities to adapt their product development, procurement strategies, and cybersecurity governance to align with CRA mandates. For AI startups operating in the energy space, early compliance—or demonstrable preparation—can serve as a compelling value proposition for risk-averse clients and public procurement frameworks. It also positions these firms to avoid regulatory bottlenecks and gain preferential access to European markets.

## 2.2. Impact of Regulations on AI Development in Energy sector

This section provides a comprehensive review of the literature concerning ultra-short-term forecasting of wind speed and wind power. The focus is on methods developed to address the challenges of predicting wind energy output over very short lead times (typically ranging from a few minutes to several hours). The reviewed studies are categorized primarily based on the type of forecasting models employed. Additionally, key attributes such as input data types, evaluation metrics, and spatial scales used in the analyses are summarized. The development, deployment, and operationalization of artificial intelligence (AI) technologies within the European energy sector are increasingly shaped by an evolving framework of EU regulations. These laws collectively establish the conditions under which AI can be safely and responsibly integrated into the energy value chain. This section provides a granular analysis of the implications of this regulatory environment on the **generation segment**, encompassing both centralized and distributed energy production systems. The discussion covers applicable legal instruments, sector-specific compliance challenges, and emerging opportunities, including the potential for regulatory enablers. Additionally, areas of legal ambiguity are highlighted, particularly where regulation has not yet matured to address the full complexity of AI applications.

AI technologies in energy generation are primarily employed to optimize performance, enhance safety, and support the integration of renewable resources. Examples include predictive maintenance algorithms in thermal plants, machine learning models for wind and solar output forecasting, and intelligent control systems for load balancing and fault detection. Generation assets are typically operated by large utility companies or independent power producers (IPPs), which are already subject to stringent technical, safety, and reliability standards.

Power generation facilities, particularly those contributing to national grid stability or operating hazardous assets (e.g., nuclear or hydroelectric plants), fall under the EU's definition of critical infrastructure. AI systems integrated into these settings—such as those supporting reactor regulation, thermal dispatch optimization, or turbine protection mechanisms—are likely to be classified as high-risk under the AI Act [8]. Compliance with this classification mandates comprehensive risk management, ex ante conformity assessments, documentation of technical robustness, and in certain cases, third-party certification. While these requirements may introduce delays and additional compliance costs for AI developers, they align with the existing safety-oriented certification culture prevalent in the generation sector. Nonetheless, a critical challenge lies in the current absence of standardized benchmarks for evaluating the accuracy, robustness, and reliability of AI systems in operational control settings. Although AI deployments in power generation are primarily industrial in nature and often process non-personal data (e.g., sensor and equipment diagnostics), certain scenarios trigger GDPR applicability. These include AI systems involved in workforce scheduling, biometric access control, or the management of customer-facing distributed energy resources (e.g., residential solar-battery systems). In such cases, AI applications must adhere to GDPR principles, including lawful data processing, data minimization, transparency, and data subject rights. Energy organizations must therefore implement robust data governance practices, particularly when AI technologies interface with personal or sensitive information.

Large energy generators are classified as essential entities under the NIS2 Directive, which imposes heightened obligations regarding cybersecurity risk

management, incident reporting, and business continuity [7]. The deployment of AI in these contexts—for instance, through predictive maintenance tools connected to external cloud analytics platforms—requires the identification, evaluation, and mitigation of associated cybersecurity threats, such as data breaches, unauthorized access, or system manipulation. Similarly, the Network Code on Cybersecurity, while primarily focused on transmission and distribution operators, extends its influence to generation assets that are integral to cross-border electricity flows. AI-based controllers, governors, and automated voltage regulators may thus fall under cybersecurity risk assessments, necessitating robust digital safeguards and potentially leading to sector-specific hardening practices, such as emergency override systems for AI anomalies. A major compliance hurdle is the seamless integration of AI systems across information technology (IT) and operational technology (OT) environments. Many generation facilities already adhere to safety-critical standards like IEC 61508; aligning these legacy frameworks with new AI and cybersecurity obligations presents a complex dual-compliance challenge.

Although the EU Cybersecurity Act does not mandate specific certifications for AI systems, it lays the foundation for sector-specific assurance schemes. Generation companies may voluntarily pursue certifications under schemes aligned with ISO/IEC 27001 for IT systems or IEC 62443 for industrial automation security. Such certifications, especially those classified under “High” assurance levels, could be leveraged to demonstrate due diligence in securing AI-driven assets. Forward-looking utilities may adopt these certifications preemptively to improve trust, reduce liability exposure, or benefit from favorable insurance terms [10]. Moreover, compliance with the AI Act’s *human oversight* requirement necessitates operational changes. Engineers and operators must be able to understand and, if necessary, override AI decisions. This calls for transparent, explainable AI systems and appropriate training for control room personnel. Given the traditionally conservative culture within power generation, where safety and reliability take precedence over innovation, achieving this level of integration requires significant organizational adaptation. Regulation may act as a catalyst by enforcing logging, transparency, and auditability, thereby demystifying AI

systems and facilitating their gradual acceptance [9].

Beyond compliance obligations, EU regulatory frameworks also contain provisions that can enable innovation. The AI Act, for instance, promotes the use of *regulatory sandboxes*—controlled environments in which AI systems can be tested under supervisory guidance. While not compulsory, such initiatives are encouraged to foster experimentation with emerging AI technologies, especially where the risk classification is uncertain or where the technology is novel. Several EU Member States, including the Netherlands [8] and Germany [4], have established sector-specific sandbox programs for smart grid and energy system innovation. These platforms allow companies to deploy AI-driven solutions such as virtual power plants or decentralized control platforms without immediate exposure to regulatory penalties. In doing so, they help validate technologies, inform future regulations, and provide clearer compliance pathways for full-scale implementation.

## Conclusion

In summary, the integration of AI into energy generation systems is subject to a multifaceted regulatory framework encompassing product-level security (CRA), data protection (GDPR), operational cybersecurity (NIS2 and Network Code), and AI-specific governance (AI Act). While these laws introduce necessary safeguards, they also present technical, legal, and operational challenges that stakeholders must address through proactive compliance strategies. At the same time, emerging instruments such as certification schemes and sandboxes offer valuable pathways for innovation and risk mitigation. As regulatory clarity improves and technical standards mature, AI is poised to become a transformative tool in energy generation—provided it is deployed with the rigor and transparency demanded by the EU's legislative landscape.