Comparative Analysis of AI Regulations: EU AI Act, US Approach, and China's Framework (2025)

Executive Summary

As of 2025, the global landscape of AI regulation has evolved into three distinct approaches: the European Union's comprehensive risk-based regulatory framework (AI Act), the United States' sectoral and standards-driven approach, and China's evolving regulatory framework focused on national security and social stability. This report provides a detailed comparison of these regulatory approaches, highlighting their similarities, differences, enforcement mechanisms, and the criticisms raised by experts and industry stakeholders.

1. The European Union's AI Act

1.1 Regulatory Framework and Implementation Status

The EU AI Act (Regulation (EU) 2024/1689) represents the world's first comprehensive legal framework specifically designed for artificial intelligence. As noted by the European Commission, "The AI Act (Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence) is the first-ever comprehensive legal framework on AI worldwide. The aim of the rules is to foster trustworthy AI in Europe." [1]

The implementation of the AI Act is occurring on a phased timeline, with different provisions taking effect at various points through 2025-2027. According to the European Parliament, "The act's rules kick in on a rolling basis over the next few years, with the first set of prohibitions coming into effect in February 2025." [2]

1.2 Risk-Based Classification System

The cornerstone of the EU approach is its risk-based classification system, which categorizes AI systems into four risk levels:

1. **Unacceptable Risk**: Banned applications include:
    - Harmful AI-based manipulation and deception
    - Social scoring systems
    - Certain biometric identification practices (with limited exceptions for law enforcement)
    - Real-time remote biometric identification in publicly accessible spaces [1]
2. **High Risk**: Regulated applications include:
    - AI in critical infrastructure (transport, energy)
    - AI in education determining access to education
    - AI in employment (CV-sorting software)
    - AI for credit scoring and essential services

    - AI in law enforcement and border control [1]
3. **Limited Risk**: Systems requiring specific transparency obligations (e.g., chatbots)
4. **Minimal Risk**: Systems subject to minimal requirements

As the European Parliament explains: "AI systems that negatively affect safety or fundamental rights will be considered high risk and will be divided into two categories: 1) AI systems that are used in products falling under the EU's product safety legislation; 2) AI systems falling into specific areas that will have to be registered in an EU database." [2]

1.3 Enforcement Mechanisms

The EU AI Act establishes a multi-layered enforcement framework:

- **National Competent Authorities**: Each member state designates authorities responsible for enforcement
- **European AI Office**: Established to coordinate implementation across the EU
- **Market Surveillance**: Ongoing monitoring of AI systems post-deployment
- **Fines**: Up to 7% of global turnover or €30 million for serious violations [1]

The European Commission has also launched the "AI Pact," a voluntary initiative "that seeks to support the future implementation, engage with stakeholders and invite AI providers and deployers from Europe and beyond to comply with the key obligations of the AI Act ahead of time." [1]

1.4 Criticisms and Industry Concerns

Despite its comprehensive nature, the EU AI Act faces several criticisms:

- **Innovation Concerns**: Industry groups argue the strict regulations may stifle AI innovation in Europe compared to more permissive environments
- **Implementation Challenges**: Concerns about inconsistent enforcement across member states
- **Definition Issues**: Critics note the AI definition may be too broad, potentially capturing systems not traditionally considered AI
- **Generative AI Ambiguity**: Some experts argue the transparency requirements for generative AI don't adequately address specific risks [3]

As noted in industry commentary, "While the EU AI Act represents a landmark achievement in AI regulation, its strict requirements may place European companies at a competitive disadvantage globally, particularly against US and Chinese counterparts operating in less regulated environments." [3]

2. United States AI Regulatory Approach

2.1 Current Regulatory Framework

Unlike the EU's comprehensive approach, the US has adopted a more fragmented, sectoral regulatory strategy. As NIST explains: "NIST promotes innovation and cultivates trust in the design, development, use and governance of artificial intelligence (AI) technologies and systems in ways that enhance economic security, competitiveness, and quality of life." [4]

The US approach centers around:

- **Voluntary Frameworks**: Primarily the NIST AI Risk Management Framework (AI RMF)
- **Sector-Specific Regulations**: Existing laws applied to AI in specific sectors (e.g., healthcare, finance)
- **Executive Actions**: Presidential directives guiding AI development and use

2.2 Recent Developments (2025)

In July 2025, the Trump administration released "America's AI Action Plan" and signed significant executive orders that represent a shift from the previous administration's approach. As reported: "President Trump has directed the federal government to prioritize the advancement of secure software development across all systems and platforms." [5]

Key elements of the 2025 US approach include:

- **Focus on National Security**: Prioritizing protection against foreign cyber threats, particularly from China
- **Post-Quantum Cryptography**: Directing agencies to adopt next-generation cryptographic standards
- **NIST Leadership**: "By August 1, this year, the Secretary of Commerce, acting through the director of National Institute of Standards and Technology (NIST), shall establish a consortium with industry at the National Cybersecurity Center of Excellence (NCCoE) to develop guidance" [5]
- **Refocused AI Cybersecurity**: Shifting emphasis from censorship to vulnerability management
- **Limiting Sanctions**: Restricting cyber sanctions to foreign malicious actors only [5]

2.3 Enforcement Mechanisms

The US enforcement approach differs significantly from the EU:

- **Existing Agency Authority**: FTC, FDA, and other agencies applying existing laws to AI
- **Voluntary Compliance**: Emphasis on industry self-regulation and standards adoption
- **Sector-Specific Enforcement**: Different rules and enforcement mechanisms across sectors
- **Limited Federal Legislation**: No comprehensive federal AI law, though some states have enacted AI regulations [6]

As noted by experts: "The US relies on existing federal laws and guidelines to regulate AI but aims to introduce AI legislation and a federal regulation authority." [6] However, as of mid-2025, comprehensive federal legislation has not been enacted.

2.4 Criticisms and Industry Concerns

The US approach faces its own set of criticisms:

- **Regulatory Fragmentation**: Lack of consistency across states and sectors creates compliance challenges
- **Enforcement Gaps**: Existing laws weren't designed for AI, creating enforcement challenges
- **International Competitiveness**: Some argue the US approach doesn't provide sufficient guardrails compared to the EU, potentially damaging international partnerships

- **Innovation vs. Protection**: Critics argue the current approach prioritizes innovation at the expense of adequate protections [7]

Industry voices note: "The US approach creates significant uncertainty for businesses operating across multiple jurisdictions, as they must navigate a patchwork of state laws and sector-specific regulations without clear federal guidance." [7]

3. China's AI Regulatory Framework

3.1 Current Regulatory Landscape

China has developed a comprehensive but evolving AI regulatory framework centered around several key laws:

- **Cybersecurity Law (CSL)**: Originally enacted in 2016, with amendments proposed in 2025
- **Data Security Law (DSL)**: Enacted in 2021
- **Personal Information Protection Law (PIPL)**: Enacted in 2021
- **Interim Measures for Generative AI**: Implemented in 2023, with additional rules in 2025 [8]

As explained by China Briefing: "Originally enacted in 2016, the CSL is one of the three pillar laws of China's data protection and cybersecurity regime, alongside the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), both of which were passed in 2021." [8]

3.2 Recent Developments (2025)

In 2025, China has advanced several regulatory initiatives:

- **Cybersecurity Law Amendments**: The Cyberspace Administration of China (CAC) issued "new draft amendments to the Cybersecurity Law (CSL) for public comment" on March 28, 2025 [8]
- **AI-Generated Content Labeling**: "On March 14, 2025, the Cyberspace Administration of China ("CAC") released draft rules on AI-generated content labeling that will take effect on September 1, 2025." [9]
- **Regulations on Network Data Security Management**: Took effect on January 1, 2025 [8]

The 2025 amendments address previous criticisms that "the CSL has often been accused of being outdated —particularly due to its significantly lower fines compared to those outlined in the DSL and PIPL." [8]

3.3 Enforcement Mechanisms

China's enforcement approach is characterized by:

- **Centralized Authority**: The Cyberspace Administration of China (CAC) serves as the primary regulatory body
- **Stricter Penalties**: Amendments introduce "harsher penalties and clearer enforcement mechanisms, ensuring that violations result in meaningful consequences" [8]
- **Proactive Monitoring**: Extensive monitoring of AI systems and content
- **National Security Focus**: Enforcement heavily prioritizes national security considerations [9]

As noted in regulatory analysis: "These innovative enforcement mechanisms demonstrate China's evolving regulatory strategy, which aims to strike a balance between encouraging AI innovation and maintaining control over potentially destabilizing technologies." [8]

3.4 Criticisms and Industry Concerns

China's approach faces significant international criticism:

- **Human Rights Concerns**: Critics argue the framework enables surveillance and social control
- **Lack of Transparency**: Regulatory processes are often opaque
- **Protectionism**: Some provisions appear designed to favor domestic companies
- **Innovation Constraints**: Strict content controls may limit creative AI applications [10]

International observers note: "China's regulatory approach prioritizes state control and social stability over individual rights and innovation, creating a fundamentally different AI ecosystem compared to Western approaches." [10]

4. Comparative Analysis

4.1 Key Similarities

Despite their differences, the three regulatory approaches share some common elements:

- **Risk-Based Elements**: All three frameworks incorporate some form of risk assessment, though the EU's is most formalized
- **Focus on Transparency**: All require some level of transparency for AI systems, particularly generative AI
- **Data Protection Integration**: All frameworks integrate with broader data protection regimes
- **Adaptation to Generative AI**: All have developed specific rules for generative AI systems [11]

As noted in comparative research: "While the EU, US, and China have taken different paths to AI regulation, they share common concerns about transparency, accountability, and the need to address specific risks posed by advanced AI systems." [11]

4.2 Key Differences

Dimension	EU AI Act	US Approach	China's Framework
Regulatory Philosophy	Precautionary principle, rights protection	Innovation-first, sectoral regulation	National security, social stability
Legal Structure	Comprehensive horizontal law	Fragmented sectoral approach	Multiple laws with central oversight
Enforcement	Formal regulatory bodies, significant fines	Existing agencies, voluntary frameworks	Centralized authority, strict penalties
Generative AI	Transparency requirements	Sector-specific guidelines	Content labeling, strict content controls
International Alignment	Seeks global influence through regulatory standards	Limited international coordination	Primarily domestic focus

4.3 Enforcement Mechanisms Comparison

- **EU**: Establishes formal regulatory bodies at national and EU levels with significant fines (up to 7% of global turnover). Features a structured market surveillance system and mandatory conformity assessments for high-risk systems.
- **US**: Relies on existing regulatory agencies applying current laws to AI applications. Emphasizes voluntary standards and industry self-regulation. Enforcement is fragmented across sectors with varying approaches.
- **China**: Centralized enforcement under the CAC with significant penalties. Focuses on proactive monitoring and national security considerations. Recent amendments aim to "strike a balance between encouraging AI innovation and maintaining control over potentially destabilizing technologies." [8]

4.4 Criticisms Comparison

- **EU Criticisms**: Overly restrictive, may stifle innovation, complex compliance requirements, inconsistent implementation across member states
- **US Criticisms**: Regulatory gaps, fragmented approach, insufficient protections, lack of clear federal guidance
- **China Criticisms**: Human rights concerns, lack of transparency, protectionism, excessive state control, innovation constraints

5. Expert and Industry Perspectives

5.1 Expert Opinions

Experts generally agree that the regulatory divergence creates significant challenges for global AI development:

"The global regulatory landscape for AI is becoming increasingly fragmented, with the EU, US, and China developing fundamentally different approaches. This fragmentation creates compliance challenges for multinational companies and may lead to a 'splinternet' for AI technologies." [12]

Some experts advocate for greater international coordination: "While each jurisdiction has legitimate reasons for its approach, the growing divergence in AI regulation threatens to undermine global cooperation on AI safety and creates unnecessary barriers to innovation." [13]

5.2 Industry Perspectives

Industry responses reflect the practical challenges of navigating these different frameworks:

- **Tech Companies**: Express concerns about the compliance burden of multiple, sometimes contradictory, regulatory regimes
- **Startups**: Particularly concerned about the EU's strict requirements, which they argue create barriers to entry
- **Financial Sector**: Focus on the challenges of applying AI regulations to financial services across different jurisdictions

- **Healthcare Sector**: Concerned about inconsistent approaches to medical AI applications [14]

As noted by industry representatives: "The lack of regulatory harmonization is one of the biggest challenges facing AI developers today. Companies must navigate three fundamentally different regulatory environments, each with its own requirements and enforcement mechanisms." [14]

6. Conclusion

As of 2025, the EU, US, and China have established three distinct approaches to AI regulation that reflect their differing values, priorities, and governance models:

1. **The EU** has implemented the world's first comprehensive AI law with a risk-based approach focused on fundamental rights protection.
2. **The US** has adopted a more fragmented, innovation-focused approach centered around voluntary standards and sectoral regulation, with recent executive actions emphasizing national security.
3. **China** has developed a centralized regulatory framework focused on national security and social stability, with recent amendments strengthening enforcement mechanisms.

These differing approaches create significant challenges for global AI development and deployment. While each framework addresses legitimate concerns, the growing regulatory divergence threatens to fragment the global AI ecosystem and create unnecessary barriers to innovation. Future developments may see increased efforts at regulatory cooperation, but as of mid-2025, the three approaches remain fundamentally distinct.

References

[1] European Commission. "Regulatory Framework on AI." Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[2] European Parliament. "EU AI Act: first regulation on artificial intelligence." June 1, 2023 (updated February 19, 2025). https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[3] White & Case LLP. "AI Watch: Global regulatory tracker - European Union." May 29, 2025. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union

[4] National Institute of Standards and Technology. "Artificial Intelligence." https://www.nist.gov/artificial-intelligence

[5] Industrial Cyber. "Trump executive order rewrites US cybersecurity playbook, targets foreign threats and federal bloat." June 9, 2025. https://industrialcyber.co/regulation-standards-and-compliance/trump-executive-order-rewrites-us-cybersecurity-playbook-targets-foreign-threats-and-federal-bloat/

[6] White & Case LLP. "AI Watch: Global regulatory tracker - United States." July 21, 2025. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

[7] Mind Foundry. "AI Regulations around the World - 2025." January 25, 2024. https://www.mindfoundry.ai/blog/ai-regulations-around-the-world

[8] China Briefing. "China's Cybersecurity Law Amendments 2025: Second Draft." April 1, 2025. https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/

[9] White & Case LLP. "AI Watch: Global regulatory tracker - China." May 29, 2025. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china

[10] Carnegie Endowment. "China's AI Regulations and How They Get Made." July 10, 2023. https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en

[11] Brookings Institution. "The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment." April 25, 2023. https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/

[12] Oliver Patel. "Global AI Law Snapshot: EU, China and U.S.A." February 4, 2025. https://oliverpatel.substack.com/p/global-ai-law-snapshot-eu-china-and

[13] EH4S. "Comparative Analysis of AI Development Strategies: A Study of China's Ambitions and the EU's Regulatory Framework." September 20, 2024. https://eh4s.eu/publication/comparative-analysis-of-ai-development-strategies-a-study-of-chinas-ambitions-and-the-e-us-regulatory-framework

[14] Kennedy's Law. "Key insights into AI regulations in the EU and the US: navigating the evolving landscape." January 21, 2025. https://kennedyslaw.com/en/thought-leadership/article/2025/key-insights-into-ai-regulations-in-the-eu-and-the-us-navigating-the-evolving-landscape/