

FROM EUROPE'S RIGHTS-BASED AI REGULATION TO KOREA'S INNOVATION-ORIENTED FRAMEWORK: DIVERGING PHILOSOPHIES IN GLOBAL DIGITAL AND AI GOVERNANCE

BONGCHUL KIM

bong625@hufs.ac.kr

Bongchul Kim is Professor at the Division of International Studies at Hankuk University of Foreign Studies (South Korea). He obtained his Bachelor of Laws and Master of Laws from Hufs and received his Ph.D. in Laws from King's College London with the Overseas Research Scholarship awarded by the UK government. He previously served as President of the Korean Society of Contemporary European Studies (KSCES) and as Director of the Hufs EU Institute. He currently serves as Director of the Hufs Jean Monnet EU Centre, Hufs Polar Research Centre, and Director of the Seoul Institute of Global Affairs (SIGA).

Abstract

This article examines the divergent regulatory philosophies shaping global digital and AI governance by comparing the European Union's rights-based regulatory model, Italy's enforcement-oriented domestic adaptation, and Korea's innovation-oriented AI framework. It argues that the EU has emerged as a global regulatory power through its Digital Services Act, Digital Markets Act, and Artificial Intelligence Act, embedding principles such as human dignity, transparency, accountability, and fundamental rights protection into the architecture of digital governance. Conceptually, the article situates the EU's regulatory influence within the framework of the Brussels Effect, showing how European digital and AI standards extend beyond the EU market and shape broader international governance debates. Empirically, it analyzes the EU AI Act's risk-based regulatory structure and Italy's national AI legislation, which deepens EU regulatory logic through digital humanism, criminal liability, watermarking obligations, and strong institutional oversight. The article then turns to Korea's AI Basic Act, highlighting its more flexible and innovation-oriented approach. Unlike the EU and Italian models, Korea places greater emphasis on industrial development, data utilization, and adaptive governance while selectively incorporating risk-based regulatory elements. Rather than treating these models as mutually exclusive, the article argues that they reveal complementary pathways in global AI governance. It concludes that future Korea-EU cooperation should move beyond technical regulation and address the deeper philosophical challenge of reconciling human-centered accountability with technological innovation.

Keywords

AI governance, EU AI Act, Brussels Effect, Korea AI Basic Act, Digital humanism.

Resumo

Este artigo analisa as filosofias regulatórias divergentes que moldam a governação global no domínio digital e da IA, comparando o modelo regulatório da União Europeia, baseado nos direitos, a adaptação nacional da Itália, orientada para a aplicação da lei, e o quadro de IA da Coreia, orientado para a inovação. Defende que a UE se tornou uma potência regulatória global através da sua Lei dos Serviços Digitais, da Lei dos Mercados Digitais e da Lei da Inteligência Artificial, incorporando princípios como a dignidade humana, a transparência, a responsabilização e a proteção dos direitos fundamentais na arquitetura da governação



digital. Conceitualmente, o artigo situa a influência regulatória da UE no âmbito do «Efeito Bruxelas», mostrando como as normas europeias em matéria de digital e IA se estendem para além do mercado da UE e moldam debates mais amplos sobre a governação internacional. Empiricamente, analisa a estrutura regulatória baseada no risco da Lei da IA da UE e a legislação nacional italiana em matéria de IA, que aprofunda a lógica regulatória da UE através do humanismo digital, da responsabilidade criminal, das obrigações de marcação digital e de uma forte supervisão institucional. O artigo volta-se, em seguida, para a Lei Básica sobre IA da Coreia, destacando a sua abordagem mais flexível e orientada para a inovação. Ao contrário dos modelos da UE e da Itália, a Coreia dá maior ênfase ao desenvolvimento industrial, à utilização de dados e à governação adaptativa, ao mesmo tempo que incorpora seletivamente elementos regulamentares baseados no risco. Em vez de tratar estes modelos como mutuamente exclusivos, o artigo defende que eles revelam vias complementares na governação global da IA. Conclui que a futura cooperação entre a Coreia e a UE deve ir além da regulamentação técnica e abordar o desafio filosófico mais profundo de conciliar a responsabilização centrada no ser humano com a inovação tecnológica.

Palavras-chave

governação da IA, Lei da UE sobre a IA, Efeito Bruxelas, Lei Básica da Coreia sobre a IA, humanismo digital.

How to cite this article

Kim, Bongchul (2026). From Europe's Rights-Based AI Regulation to Korea's Innovation-Oriented Framework: Diverging Philosophies in Global Digital and AI Governance. *Janus.net, e-journal of international relations*. Thematic Dossier – Geopolitics of Anxiety: Ideology, Identity, and (Un)Bordering in Contemporary Europe and Asia, VOL. 17 Nº. 1, TD3, September 2026, pp. 63-82. DOI <https://doi.org/10.26619/1647-7251.DT0626.4>

Article submitted on March 30, 2026 and accepted on May 10, 2026.





FROM EUROPE'S RIGHTS-BASED AI REGULATION TO KOREA'S INNOVATION-ORIENTED FRAMEWORK: DIVERGING PHILOSOPHIES IN GLOBAL DIGITAL AND AI GOVERNANCE¹

BONGCHUL KIM

AI Governance in a Global Context: EU Leadership and Korea's Emerging Role

The development of intelligent technologies, including Artificial Intelligence (AI), is advancing at an unprecedented pace, significantly expanding its influence across economic, social, and security domains. Governments and corporations worldwide are actively investing in AI development and deployment to prepare for this emerging era, while simultaneously anticipating and addressing the social challenges that such technologies may generate. As a result, AI has become a key arena of both international competition and cooperation. States are striving to secure technological superiority while also establishing institutional frameworks to mitigate risks such as privacy violations, algorithmic bias, and misuse. Consequently, AI has emerged as one of the most critical factors shaping future economic growth, governance structures, and security environments.

Major countries are approaching AI not only as an engine of economic innovation but also as a strategic asset in national security. Regulatory policies are expanding as governments seek to protect domestic industries and maintain competitiveness, recognizing that inadequate responses could undermine long-term economic performance (National Information Society Agency, 2023). In the security domain, AI is increasingly viewed as a core component of future warfare. The United States has emphasized its importance in maintaining strategic dominance in a rapidly evolving technological landscape (Walch, 2021), while China has projected the emergence of AI-driven warfare in its national defense strategies (Cha, 2021). Europe, through frameworks such as NATO, is also investing in the security applications of AI. These developments demonstrate that AI is not confined to a single domain but is instead reshaping multiple dimensions of global governance and competition.

In this context, the European Union (EU) introduced the Artificial Intelligence Act (EU AI Act) in 2021, the world's first comprehensive legislative attempt to regulate AI, which

¹ This study is supported by Ministry of Education, the National Research Foundation of Korea(NRF-2022S1A5C2A02091292), and 2026 Hankuk University of Foreign Studies academic research fund.



was ultimately finalized in 2024. Unlike approaches that focus primarily on technological development and economic utilization, the EU sought to establish a regulatory framework ensuring the safe and ethical use of AI in everyday life. This initiative represents a significant milestone in global AI governance and reinforces the EU's role as a "normative power" shaping international standards. As AI becomes increasingly embedded in daily life, the need for such regulatory frameworks has grown more urgent, given the potential for unintended social consequences. Therefore, analyzing the EU AI Act and its regulatory principles provides an essential foundation for understanding the evolving landscape of AI governance.

At the same time, effective AI governance requires active international cooperation, and Korea has begun to play an important role in this process. Korea has recently enacted its own Framework Act on Artificial Intelligence and is promoting national strategies to support AI innovation and industrial growth. As one of the countries that has followed the EU in establishing a legal framework for AI, Korea is well positioned to engage in global discussions and collaborative efforts. In particular, given the similarities in regulatory orientation between Korea and Europe, there is strong potential for deeper cooperation.

This article begins with an introduction to the EU's digital regulatory framework, focusing on the enactment and key features of the AI Act, and then examines Korea's legislative response to AI governance. Ultimately, it argues that sustained legal and policy cooperation between Korea and Europe in the field of digital and AI regulation is both necessary and desirable for addressing shared challenges and promoting responsible technological development. Such cooperation will contribute to the harmonization of international standards and enhance mutual capacity to respond effectively to the rapidly evolving risks and opportunities associated with AI.

EU Regulatory Power in the Digital and AI Economy: The Brussels Effect and Global Implications

The Digital Economy, EU Regulatory Power, and the Brussels Effect

The digital economy now constitutes a significant portion of the global economy, and its influence is expected to expand further in the coming years. In particular, as economic and social activities shifted online during the global spread of COVID-19, e-commerce and digital markets experienced rapid growth. As a result, the digital economy has become an essential part of everyday life and a fundamental domain of modern markets. In response, societies are transitioning toward digital-based systems, necessitating corresponding transformations in national policies and institutional frameworks (European Central Bank, 2020). Accordingly, major countries are striving not only to address challenges arising from digitalization but also to secure a competitive advantage in the global economy.

As of 2020, the size of the digital market had reached a level comparable to the gross domestic product of G7 countries. Core elements of the digital environment—such as data utilization, hyper-connectivity, and efficient software supply—have become essential



inputs across industries, similar to labor or electricity (World Economic Forum, 2020). At the same time, advanced technologies such as AI and big data are increasingly integrated into economic activities. Governments are therefore expanding policy frameworks to incorporate digital trade and establish relevant norms (Park, J. H., 2024).

In this context, the European Union (EU) has played a leading role in shaping the digital economy through regulatory and policy initiatives. The EU has promoted digital transformation across industries while embedding these developments within a broader normative framework aimed at protecting core values such as data protection and fair competition (Choi, S. K., 2022). The urgency of these efforts increased significantly following COVID-19, which accelerated both digital adoption and policy implementation (Lee & Kim, 2022).

The EU's digital strategy builds on its long-standing efforts toward economic integration. Beginning with the Europe 2020 strategy and the Digital Agenda for Europe, the European Commission introduced the Digital Single Market Strategy in 2015 to eliminate barriers to digital economic activity and establish a unified regulatory environment (European Commission, 2015). The Digital Single Market aims to ensure the free movement of goods, services, capital, and people, while enabling individuals and businesses to operate online under conditions of fair competition and strong data protection. Within this framework, the General Data Protection Regulation (GDPR) has been a key instrument in strengthening data governance (Noh, 2023).

The EU has continued to advance its digital strategy in recent years. In July 2024, following the reappointment of Ursula von der Leyen, the EU introduced its Political Guidelines 2024–2029, emphasizing the deepening of the Digital Single Market and the promotion of AI-driven growth (European Commission, 2024a; Jang et al., 2024). In this evolving landscape, cooperation between Korea and Europe is becoming increasingly important. Given their shared emphasis on innovation, data protection, and fair competition, closer collaboration can contribute to the harmonization of regulatory standards, reduce fragmentation, and enhance mutual competitiveness in the global digital economy.

A key concept for understanding the global influence of EU regulation is the Brussels Effect, first introduced by Anu Bradford. This concept refers to the phenomenon whereby EU regulatory standards extend beyond its borders and become de facto global norms (Bradford, 2020). The EU's ability to shape international regulatory environments stems not from coercion, but from its capacity to set rules that others adopt voluntarily (Bradford, 2012). This influence spans multiple domains, including data privacy, consumer protection, competition policy, and digital governance.

At its core, the Brussels Effect is driven by the size and attractiveness of the EU's internal market. As one of the world's largest consumer markets, the EU incentivizes multinational corporations to comply with its regulations in order to maintain market access. Once these standards are adopted, firms often apply them globally to ensure efficiency and legal consistency. This process differs from traditional regulatory diffusion in that it is based on market incentives rather than formal international agreements, making voluntary compliance a defining feature.



The Brussels Effect is closely linked to the concept of normative power, which refers to the ability to shape global norms by defining what is considered legitimate or appropriate (Manners, 2002). In this regard, the EU functions as a normative power by exporting its regulatory frameworks. Bradford further distinguishes between the “de facto” Brussels Effect, where firms voluntarily adopt EU standards, and the “de jure” Brussels Effect, where such standards are formally incorporated into domestic legal systems (Bradford, 2021).

Recent developments suggest that the Brussels Effect is increasingly evolving into a de jure phenomenon, as countries adopt EU-style regulations into their own legal frameworks (Oh, C. R., 2023). A representative example is the General Data Protection Regulation (GDPR), which has established itself as a global benchmark since its implementation in 2018. By introducing strengthened individual rights and obligations for data processors—such as the right to erasure and data portability—and applying extraterritorially to organizations handling EU citizens’ data, the GDPR has significantly expanded the global reach of EU digital norms. As a result, countries including Japan and Korea, as well as multinational corporations, have increasingly aligned their regulatory frameworks with EU standards.

EU Digital Market Regulation: DSA and DMA

The regulation of online platforms has emerged as a central issue in the global digital economy. The growing dominance of large technology companies has raised concerns about market concentration, unfair competition, and barriers to entry for smaller firms. While these platforms generate efficiency gains and consumer benefits, their “winner-takes-all” dynamics may limit innovation and reduce long-term market dynamism (Choi, N. S. H., 2022). In addition, issues such as data privacy, algorithmic transparency, and the spread of illegal or harmful content have intensified calls for regulatory intervention. As a result, governments around the world are actively debating the scope and form of digital market regulation. Within the EU, member states are required to implement common regulatory frameworks; however, differences in administrative capacity and institutional readiness have led to uneven enforcement across countries.

The EU has taken a leading role in addressing these challenges through proactive regulatory strategies. A key milestone was the 2017 Google Shopping case, in which the European Commission imposed a €2.42 billion fine on Google for abusing its dominant position by favoring its own services. This case demonstrated the limitations of traditional competition law in dealing with digital platforms and highlighted the need for more targeted regulatory frameworks. In response, the EU has progressively strengthened its regulatory approach to address structural issues in digital markets (Kang, 2019). At the same time, member states have been required to adapt their domestic enforcement systems, although the level of implementation and effectiveness has not been uniform across the EU.

Building on this experience, the EU introduced a comprehensive legislative framework in December 2020 through the Digital Services Act (DSA) and the Digital Markets Act



(DMA). These laws, collectively known as the Digital Services Act Package, aim to address systemic problems in the platform economy, including lack of transparency, data protection concerns, and unfair business practices (European Commission, 2016). They also reflect the EU's broader objective of securing digital sovereignty and reducing dependence on non-European technology firms (Echikson, 2024; Shin & Kim, 2023). Although these regulations are directly applicable across the EU, variations in national enforcement—particularly among Eastern European countries—continue to influence their practical implementation.

The Digital Services Act focuses on creating a safer and more transparent online environment. It establishes clear obligations for online platforms regarding the removal of illegal content, the protection of users, and the transparency of algorithms and advertising systems. Platforms are required to implement effective content moderation mechanisms and to provide users with information about how decisions are made. In particular, very large online platforms are subject to enhanced responsibilities due to their systemic impact on society. These measures are expected to improve trust, accountability, and predictability in digital ecosystems (Lee, K. I., 2024).

The Digital Markets Act, in contrast, targets structural competition issues by regulating "gatekeeper" platforms—firms that control key access points to digital markets and possess significant market power. The DMA imposes ex ante obligations on these firms, including requirements to ensure interoperability, enable data portability, and refrain from self-preferencing practices. This proactive regulatory approach represents a departure from traditional ex post competition enforcement and allows regulators to prevent anti-competitive behavior before it occurs (Yang, J. W., 2024).

Taken together, the DSA and DMA establish a comprehensive regulatory framework that addresses both content governance and market structure in the digital economy. They aim to protect consumers, ensure fair competition, and foster innovation while reinforcing the EU's role as a global regulatory leader. As these laws apply to all firms operating in the European market, including multinational corporations, their impact is likely to extend beyond Europe through mechanisms similar to the Brussels Effect. At the same time, internal variations among member states continue to affect the consistency and effectiveness of enforcement. Consequently, the EU's digital regulations are expected to play a central role in shaping the future global governance of digital markets (Choi, Y. S., 2022).

The EU AI Act: Background, Structure, and Global Implications

In 2021, the European Commission introduced a legislative proposal to regulate artificial intelligence (AI) (European Commission, 2024a). As AI technologies became increasingly commercialized, concerns emerged regarding potential violations of personal data and fundamental rights. The proposal aimed to mitigate these risks while enhancing the trustworthiness of AI systems. At the same time, the EU sought to balance regulation with innovation by introducing complementary measures to support the development and deployment of AI technologies.



Following negotiations among the European Parliament, the European Commission, and the Council of the European Union, the Artificial Intelligence Act was formally adopted in 2024 (European Council · Council of the European Union, 2024). As the first comprehensive legal framework for AI governance, the Act has attracted global attention. While it is widely recognized as a milestone in AI regulation, some critics argue that stringent regulatory measures could potentially hinder technological innovation (Martens, 2024).

A defining feature of the EU Artificial Intelligence Act is its adoption as a “regulation” within the EU legal system. As such, it is directly applicable in all member states without requiring national implementing legislation and allows limited discretion in interpretation. This ensures uniformity and strong legal binding force across the EU. The Act thus represents a shift from earlier international approaches—largely based on non-binding guidelines—toward enforceable legal standards (Hong, 2022).

The Act establishes a comprehensive and structured regulatory framework, consisting of 13 chapters, 113 articles, and 13 annexes. Its primary objective is to protect fundamental rights—including health, safety, democracy, the rule of law, and environmental protection—from risks associated with AI systems (Article 1). It applies broadly to AI systems operating within the EU market, covering both providers and deployers, while excluding military and national security applications (Article 2). Importantly, its scope extends beyond the EU, requiring non-EU companies to comply if they wish to access the European market (European Commission, 2024b).

In terms of regulatory content, the Act introduces differentiated obligations depending on the type and risk level of AI systems. It includes transparency requirements (Chapter 4), specific provisions for general-purpose AI models such as risk management and copyright (Chapter 5), and mechanisms to promote innovation, including regulatory sandboxes designed to support startups and small and medium-sized enterprises (Chapter 6). In addition, the Act reinforces data protection standards in alignment with existing EU frameworks, ensuring consistency with broader privacy regulations (Park & Kim, 2024).

Through the AI Act, the EU aims to extend its regulatory influence globally, similar to its role in shaping international data protection standards through the GDPR (European Council · Council of the European Union, 2024). Although formally limited to the EU, the Act’s extraterritorial effects encourage foreign companies and governments to align with its standards. In this regard, the EU is actively shaping global AI governance through regulatory leadership, often described as a form of “normative diplomacy” (Yoon & Cho, 2024).

Despite its significance, the Act also faces several challenges. The rapid evolution of AI technologies makes it difficult to anticipate and regulate emerging risks effectively. Concerns have also been raised regarding the potential for overregulation to constrain innovation and reduce economic competitiveness (Martens, 2024). Additionally, information asymmetries between regulators and large technology firms may limit enforcement effectiveness.



Nevertheless, the increasing integration of AI into economic and social systems underscores the necessity of regulatory frameworks. The EU AI Act represents a comprehensive attempt to balance innovation with the protection of fundamental rights, offering an important model for future AI governance at both regional and global levels (Shim, 2024). In this context, countries such as Korea are increasingly required to respond proactively to evolving EU regulatory standards and align their domestic frameworks accordingly. Such efforts will be essential not only for maintaining access to the European market but also for enhancing international cooperation and contributing to the development of globally harmonized AI governance.

The EU AI Act and the Global Evolution of AI Governance: Risk-Based Regulation and Korea's Legislative Response

Italy's AI Regulation and the Domestic Implementation of EU Digital Governance

Italy has recently attracted significant attention for being one of the first European Union member states to incorporate the EU's artificial intelligence (AI) regulatory framework into domestic law (Linklaters, 2025; European Parliament & Council of the European Union, 2024). This development reflects a broader and ongoing process in which EU digital and AI governance norms are increasingly being translated into national legislation across member states (White & Case LLP, 2026). In this context, Italy's case is particularly notable, as it demonstrates an early and proactive alignment with the EU's evolving regulatory agenda, especially in the field of AI governance (JuLIA Project, 2025; Linklaters, 2025).

Against this backdrop, Italy has advanced one of the most stringent national frameworks for artificial intelligence regulation, positioning itself ahead of the EU Artificial Intelligence Act in terms of detailed legal enforcement (White & Case LLP, 2026; The National Law Review, 2026). The legislation, formally titled *Disposizioni e delega al Governo in materia di intelligenza artificiale*, reflects a regulatory philosophy grounded in "digital humanism," which prioritizes human dignity, rights, and safety over technological development. The law establishes a comprehensive national approach to governing AI, emphasizing that technological innovation must remain within clear ethical and legal boundaries (Linklaters, 2025).

One of the most distinctive features of the Italian AI law is the introduction of criminal liability for the misuse of AI systems (White & Case LLP, 2026; The Guardian, 2025). Individuals who use AI algorithms to endanger the physical or psychological safety of others, or to interfere with democratic processes such as elections, may face imprisonment ranging from one to five years (White & Case LLP, 2026; Linklaters, 2025). In addition, the law imposes strict obligations on generative AI outputs, requiring that synthetic content such as deepfakes be clearly labeled with visible watermarks. Non-compliance can result in administrative fines of up to 7 percent of a company's annual revenue, reflecting a strong deterrent approach to AI-related harm (Linklaters, 2025; White & Case LLP, 2026).



The legislation also places significant emphasis on transparency, human oversight, and the protection of minors. AI systems used in sensitive sectors such as employment, healthcare, education, justice, and sports must operate under strict transparency requirements and human supervision (CMS, n.d.). In particular, access to AI services by children under the age of 14 requires parental consent, strengthening safeguards for vulnerable users (The Guardian, 2025). These provisions reflect the broader objective of ensuring that AI systems remain accountable and aligned with societal values.

In the area of intellectual property and data use, the law introduces a nuanced regulatory approach (Cocuzza, 2025; Hogan Lovells, 2025). AI-generated works may be eligible for copyright protection if they reflect genuine human intellectual contribution (Cocuzza, 2025). At the same time, the use of text and data mining is permitted only under specific conditions, such as non-copyrighted materials or authorized scientific research. This framework seeks to balance innovation in AI development with the protection of existing intellectual property rights (Hogan Lovells, 2025).

Alongside regulatory measures, Italy has also introduced policies to support AI innovation and industrial growth (Jones Day, 2025). The government has authorized the creation of a state-backed venture capital fund of up to €1 billion to support companies operating in AI, cybersecurity, and telecommunications. Regulatory responsibilities have been assigned to the Digital Italy Agency (AgID) and the National Cybersecurity Agency (ACN), ensuring institutional coordination between innovation promotion and security oversight (Agenzia per l'Italia Digitale, n.d.). This dual structure reflects Italy's attempt to integrate regulation and industrial policy within a single governance framework.

Overall, Italy's AI law represents a hybrid regulatory model that combines strict legal enforcement, ethical principles centered on human rights, and active state support for technological development (Linklaters, 2025; White & Case LLP, 2026). The government under Prime Minister Giorgia Meloni has described the law as an effort to "bring innovation back within the boundaries of public interest," ensuring that AI development contributes to economic growth while safeguarding citizens' rights (The National Law Review, 2026). As one of the first comprehensive national AI regimes in Europe to align closely with the EU's regulatory direction ahead of full implementation of the AI Act, Italy's approach is likely to influence broader European and global discussions on AI governance.

The EU Risk-Based AI Regulation and Italy's National Enforcement Model

A central pillar of the EU Artificial Intelligence Act is its "risk-based approach," which serves as the core regulatory principle of the framework. Under this system, AI technologies are classified into four categories according to their potential level of risk: Unacceptable risk, High risk, Limited risk, and Minimal risk. This classification forms the structural foundation of the Act, enabling differentiated regulation in which legal obligations are proportionate to the level of risk posed by each AI system. In this sense, the EU establishes an *ex ante* regulatory model that anticipates risks in advance and assigns appropriate legal responsibilities accordingly (Y, C. S., 2024).



Based on this framework, the Act imposes differentiated obligations on providers and deployers of AI systems. High-risk systems are subject to the most stringent and comprehensive regulatory requirements, reflecting their potential impact on safety and fundamental rights. Limited-risk systems, by contrast, are primarily associated with transparency obligations. These include requirements to inform users when they are interacting with AI-generated content, thereby addressing potential informational asymmetries and enhancing user trust. Minimal-risk systems, such as spam filters and other widely used applications, are generally permitted with minimal regulatory intervention, subject only to voluntary best-practice measures aimed at ensuring safety and reliability.

At the most restrictive end of the spectrum, Chapter 2 prohibits AI systems classified as posing unacceptable risks. These systems are deemed incompatible with EU values as they may undermine human dignity, violate fundamental rights, or manipulate human behavior, and are therefore prohibited in principle under Article 5, with only narrow exceptions such as law enforcement or counter-terrorism contexts (Jeon, 2024). Chapter 3 (Articles 6–49) regulates high-risk AI systems in detail, allowing their use only under strict compliance conditions. Providers must meet extensive requirements regarding data governance, documentation, transparency, human oversight, and risk management, ensuring a high level of accountability prior to market deployment.

Annexes 1 and 3 further specify the criteria for identifying high-risk systems. In general, AI systems subject to existing EU product safety legislation are classified as high risk, requiring conformity assessments, often conducted by third parties, to ensure compliance with regulatory standards (Lee, S. Y., 2023; Mökander, J., et al., 2022). In addition, systems used in sensitive areas such as biometric identification, critical infrastructure, public services, and law enforcement are also included in the high-risk category and are subject to rigorous pre-market controls.

In contrast to the EU framework, Italy has recently adopted a more enforcement-intensive and human-centered approach through its national AI legislation. While the EU AI Act primarily establishes a harmonized regulatory architecture based on risk classification and compliance obligations, the Italian AI law complements this structure by introducing stronger deterrent mechanisms at the domestic level. Notably, it incorporates criminal liability provisions for the misuse of AI systems, including penalties for the malicious use of AI that endangers individuals or interferes with democratic processes. It also mandates explicit watermarking of synthetic content such as deepfakes and imposes significant administrative fines for non-compliance. Furthermore, Italy places stronger emphasis on direct state supervision, including parental consent requirements for minors and centralized oversight by national agencies such as the Digital Italy Agency (AgID) and the National Cybersecurity Agency (ACN). In this respect, while the EU framework is primarily preventive and harmonized in nature, the Italian approach is more punitive and enforcement-oriented, reflecting a stricter interpretation of “digital humanism.”

Overall, the EU risk-based approach represents a systematic and preventive model of AI governance aimed at embedding European values—such as human dignity, safety, and



fundamental rights—into technological regulation (Mökander, J., et al., 2022). By contrast, Italy's approach demonstrates how member states may supplement EU-level harmonization with stricter national enforcement mechanisms. Together, these developments illustrate a multi-layered governance structure in which EU-wide regulatory principles are complemented by domestic legal experimentation. As a result, the EU's regulatory framework is increasingly positioned as a global reference point for trustworthy AI governance, with implications extending beyond Europe into broader international regulatory discussions.

Diverging Paths in Global AI Governance: The EU, Italy, and Korea

As the use of AI continues to expand, various adverse effects have become increasingly apparent. Issues such as the misuse and abuse of AI in everyday life, the distortion of facts generated by AI systems, violations of privacy, and the emergence of discriminatory algorithms due to biased data have all been widely discussed (Rességuier, A., & Rodrigues, R, 2020). These challenges highlight that AI is not only a driver of innovation but also a source of significant social risks that require careful governance.

In response, there is now a broad international consensus on the need to regulate AI technologies through structured governance frameworks. A key regulatory principle is the identification and categorization of risks, followed by differentiated regulatory measures that impose stricter obligations on higher-risk systems (Kim, B. Y., 2023). However, AI governance models vary significantly across jurisdictions, reflecting differences in institutional traditions, economic priorities, and technological capabilities.

The United States represents a leading innovation-driven model, emphasizing technological leadership and flexible governance through executive orders and sectoral regulation rather than a unified legal framework (National Information Society Agency, 2024). In contrast, China adopts a more centralized and state-led approach, combining industrial promotion with strict regulatory control through laws such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (Lee, S. W., 2022). Meanwhile, the European Union (EU) has developed a comprehensive rights-based regulatory model centered on the Artificial Intelligence Act, which is grounded in a risk-based classification system and strongly oriented toward the protection of fundamental rights and the prevention of social harm.

Within this global regulatory landscape, Italy and Korea represent two distinct forms of domestic adaptation to EU-style governance. Italy, as an EU member state, has gone beyond the EU Artificial Intelligence Act by introducing a more enforcement-oriented national framework grounded in "digital humanism." Its legislation incorporates criminal liability for the misuse of AI, mandatory watermarking of synthetic content, and strict administrative penalties, alongside strong institutional oversight through national agencies. In this sense, Italy exemplifies a "deepening" of EU regulatory logic at the domestic level, particularly through stronger deterrence mechanisms and direct legal enforceability.



Korea, by contrast, reflects a different pattern of regulatory reception and adaptation. In December 2020, the Ministry of Science and ICT and the Korea Information Society Development Institute introduced the AI Ethics Guidelines, based on OECD principles and emphasizing “AI for Humanity” (Ministry of Science and ICT, 2020). Building on these soft-law foundations, Korea progressively developed legislative proposals that culminated in the enactment of the Framework Act on the Development of Artificial Intelligence and the Establishment of a Foundation for Trust (AI Basic Act), adopted on January 21, 2025 and scheduled to take effect in January 2026. The Act combines industrial promotion with risk management, including state-led AI development planning, R&D support, and the classification of “high-impact AI” subject to additional obligations (Article 2; Article 31; Article 32).

Unlike the EU model, which prioritizes fundamental rights protection through a stringent risk-based regulatory architecture, Korea places relatively greater emphasis on industrial development and innovation support. While it adopts a similar risk-based classification approach influenced by the EU framework (Kim, K. S., 2023), its regulatory intensity is comparatively more flexible, reflecting national policy priorities aimed at strengthening AI competitiveness.

When compared with the EU and Italian models, Korea occupies an intermediate position in global AI governance. The EU represents a highly structured and rights-oriented regulatory regime, Italy demonstrates an enforcement-enhanced domestic implementation of that regime, and Korea reflects a hybrid model that integrates regulatory principles with strong industrial policy objectives. This comparison highlights how global AI governance is evolving into a multi-layered system in which shared regulatory concepts—such as risk-based classification—are adapted differently depending on national and regional contexts.

Looking forward, the convergence and divergence among these models will continue to shape the trajectory of global AI governance. As AI becomes further embedded in social and economic systems, balancing innovation with accountability will remain a central policy challenge. In this regard, the EU’s emphasis on trustworthy AI, Italy’s strong enforcement-oriented adaptation, and Korea’s innovation-driven regulatory framework together illustrate the diverse pathways through which states seek to govern emerging technologies in an increasingly interconnected digital order.

Conclusion: Diverging and Bridging Regulatory Philosophies in Global AI Governance

The rapid expansion of the digital economy and the deepening integration of AI into social and economic systems have fundamentally reshaped global regulatory priorities. As this study has shown, the European Union has emerged as a leading actor in digital and AI governance through comprehensive legal instruments such as the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Artificial Intelligence Act. These frameworks go beyond traditional market regulation by embedding core normative principles—such as human dignity, transparency, accountability, and the protection of



fundamental rights—into the architecture of digital governance. In this respect, the EU functions not only as a regulatory power but also as a global standard-setter whose influence extends well beyond its borders through mechanisms such as the “Brussels Effect.”

At the same time, the EU experience demonstrates that formal regulatory harmonization does not automatically translate into uniform implementation. Despite the legal unity of EU regulations, differences in administrative capacity, institutional readiness, and policy execution continue to shape how digital and AI rules are applied in practice. This gap between formal convergence and practical divergence highlights the importance of governance capacity as a key determinant of regulatory effectiveness, even within highly integrated legal systems.

Against this background, Korea’s evolving AI governance framework, particularly the AI Basic Act, reflects a distinct regulatory philosophy. The Act imposes mandatory obligations only on high-risk AI systems such as those used in healthcare and biometric identification, while leaving most other domains to voluntary self-regulation by firms. Its enforcement structure relies primarily on corrective orders and administrative fines rather than criminal sanctions. This design reflects a deliberate policy choice to avoid excessive regulatory burden and to preserve room for innovation, responding to concerns that strict regulation could hinder industrial growth. In this sense, AI in Korea is not primarily framed as a risk to be contained, but as a strategic engine for overcoming structural challenges such as low growth and demographic decline.

Within this context, a deeper philosophical divergence emerges between Korea and Italy (representing the broader EU regulatory orientation). Italy’s recent AI legislation reflects a strong “digital humanism” approach that prioritizes digital citizenship, copyright protection, and strict accountability for AI misuse. It imposes criminal liability for harmful AI applications and emphasizes the protection of creators’ rights, particularly against unauthorized use of training data. Korea, by contrast, emphasizes data utilization, algorithmic innovation, and flexible access to information, including more permissive approaches to AI training data under the principle of fair use. This contrast reflects not only different regulatory techniques but also fundamentally different normative assumptions: Italy tends to frame AI as a domain requiring ethical containment to preserve human dignity, while Korea approaches AI as a developmental tool to maximize socio-economic transformation.

This divergence can be understood as a “philosophical time lag” between two regulatory worlds. Italy’s approach asks whether technology can remain subordinate to human rights and creative ownership, whereas Korea’s approach asks how technology can be mobilized to solve urgent structural problems. One emphasizes precaution and moral boundaries; the other emphasizes adaptability and innovation. Yet both systems also face internal tensions: overly strict regulation risks slowing innovation in Europe, while overly flexible governance raises concerns about ethical blind spots and social harm in Korea.

In this regard, the two models should not be seen as mutually exclusive, but rather as complementary reference points for constructing a more balanced global AI governance



framework. Italy's rights-centered approach offers an important reminder that technological progress must remain anchored in human dignity and cultural values. Korea's innovation-oriented approach highlights the necessity of maintaining flexibility in rapidly evolving technological environments. The challenge, therefore, lies in bridging these two logics—combining ethical constraint with adaptive innovation.

Ultimately, strengthening cooperation between Korea and the European Union will be essential not only in technological development but also in regulatory philosophy. As AI becomes increasingly embedded in everyday life, the future of governance will depend on the ability to reconcile innovation with accountability. A more integrated dialogue between the EU's rights-based regulatory tradition and Korea's innovation-driven governance model can contribute to the emergence of a more balanced global framework—one that ensures technological progress does not come at the expense of human dignity, and that human-centered values do not inhibit technological transformation.

References

- Agenzia per l'Italia Digitale. (n.d.). *Artificial intelligence*.
<https://www.agid.gov.it/en/intervention-areas/artificial-intelligence>
- Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review*, 107(1), 1–68.
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Bradford, A. (2021). *The European Union in a globalised world: The Brussels effect*. *Revue européenne du droit*, 2. <https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/>
- Cha, J. M. (2021). *Future warfare and military-technology solidarity: The militarization of artificial intelligence and civil-military fusion* (International Strategy Foresight No. 5). National Assembly Futures Institute.
<https://www.nafi.re.kr/new/report.do?articleNo=2855&mode=view>
- Choi, N. S. H. (2022). The implications of the EU Digital Markets Act and the role of competition law. *Advanced Commercial Law Review*, 100, 67–93.
- Choi, S. K. (2022). Implications of EU Directive 2019/770 and the revisions of the German Civil Code. *Foreign Law Review*, 46(1), 1–27.
<https://doi.org/10.17257/hufslr.2022.46.1.1>
- Choi, Y. S. (2022). The Digital Constitutionalism of the EU: The Digital Services Act and its implications for Korea. *Journal of EU Studies*, 64, 415–448.
<https://doi.org/10.18109/jeus.2022..64.415>
- CMS. (2026, February 17). *AI laws and regulations in Italy*.
<https://cms.law/en/int/expert-guides/ai-regulation-scanner/italy>



Cocuzza. (2025, October 29). *Italy's new AI law: What foreign businesses should know*. <https://www.cocuzza.it/en/2025/10/29/italys-new-ai-law-what-foreign-businesses-should-know/>

Echikson, B. (2024). *Demystifying Europe's Digital Markets Act*. Center for European Policy Analysis. <https://cepa.org/article/demystifying-europes-digital-markets-act/>

European Central Bank. (2020, April 28). *Beyond monetary policy: Protecting the continuity and safety of payments during the coronavirus crisis*. <https://www.ecb.europa.eu/press/blog/date/2020/html/ecb.blog200428~328d7ca065.en.html>

European Commission. (2015). *A Digital Single Market Strategy for Europe (COM(2015) 192 final)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192>

European Commission. (2016). *Synopsis report on the public consultation on the regulatory environment for platforms, online intermediaries and the collaborative economy*. <https://digital-strategy.ec.europa.eu/>

European Commission. (2021). *The Digital Services Act package*. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

European Commission. (2023). *Legal framework of EU data protection*. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

European Commission. (2024a). *AI Act*. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

European Commission. (2024b). *Europe's choice: Political guidelines for the next European Commission 2024–2029*. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

European Council & Council of the European Union. (2024). *Artificial intelligence act*. <https://www.consilium.europa.eu/en/policies/artificial-intelligence/>

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending regulations and directives (Artificial Intelligence Act)*. Official Journal of the European Union. <http://data.europa.eu/eli/reg/2024/1689/oj>

The Guardian (2025, September 18). *Italy first in EU to pass comprehensive law regulating use of AI*. <https://www.theguardian.com/world/2025/sep/18/italy-first-in-eu-to-pass-comprehensive-law-regulating-ai>

National Information Society Agency (2024). *Current status and implications of AI regulatory governance in major countries* (Intelligent Information Society Legal System Issue Report 2024-01). https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=82618&bcIdx=27063&parentSeq=27063



Hogan Lovells. (2025, October 21). *Italy's AI law: The good, the bad...and the actual substance*. <https://www.hoganlovells.com/en/publications/italys-ai-law-the-good-the-badand-the-actual-substance>

Hong, S. H. (2022). Main contents and implications of the European Union's Proposal for an Artificial Intelligence Act. *European Constitutional Law Review*, 38, 243–282. <https://doi.org/10.21592/eucj.2022.38.243>

Jang, Y. W., Oh, T. H., Lim, Y. J., & Kim, C. R. (2024). *Main contents and implications of the 2024–2029 European Commission policy agenda* (KIEP World Economy Focus No. 24-31). Korea Institute for International Economic Policy. https://www.kiep.go.kr/gallery.es?act=view&bid=0004&list_no=11467&mid=a10102030000

Jeon, W. J. (2024). Risk classification system of the EU AI Act and its implications for South Korea's AI policy. *Journal of Korea Information Law*, 28(2), 169–215.

Jones Day. (2025, October). *Italy leads the way in shaping national AI legislation within the EU*. <https://www.jonesday.com/en/insights/2025/10/italy-leads-the-way-in-shaping-national-ai-legislation-within-the-eu>

JuLIA Project. (2025, September 23). *Italy, Law No. 132/2025 on artificial intelligence*. <https://www.julia-project.eu/database/legislation/267>

Kang, J. W. (2019). Issues in the European Commission's Google AdSense case: Focusing on comparison with the Google Shopping case. *Journal of Competition*, 200, 90–99. <https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11174940>

Kim, B. Y. (2023). Trends and implications of regulatory legislation in major countries as a means of controlling artificial intelligence. *European Constitutional Law Review*, 42, 253–307.

Kim, K. S. (2023). On the legislation of AI Act: Comparing EU and US bills for algorithm and AI regulation. *Administrative Law Journal*, 70, 173–201.

Kim, H. K. (2022). Ethics-oriented and risk assessment-based criminal policy for high-risk artificial intelligence. *Korean Journal Of Criminology*, 34(1), 7–40.

Kim, J. G., Na, S. K., Jang, J. M., & Lee, S. H. (2015). *Major contents and implications of the EU Digital Single Market Strategy* (Today's World Economy No. 15-16). Korea Institute for International Economic Policy. https://www.kiep.go.kr/gallery.es?act=view&bid=0003&list_no=3281&mid=a10102010000

Kim, S. M., & An, B. W. (2023). *Current status and characteristics of international cooperation on artificial intelligence (AI)* (IT & Future Strategy 2023-10). National Information Society Agency. <https://www.nia.or.kr/common/board/Download.do?bcIdx=26239&cbIdx=25932&fileNo=1>

Lee, H. (2024). Trends in regulations targeting online platforms and Big Tech in major countries and their implications. *Journal of International Legal Affairs (ITL)*, 165, 48–90.



Lee, H. J. (2023). Consideration on the direction of AI discipline in the Korea AI Act: Focusing on the comparison of the EU AI Act regulation. *CAU Journal of Legal Studies*, 47(2), 5–42. <https://doi.org/10.22853/caujls.2023.47.2.5>

Lee, H. Y. (2024). The Brussels Effect and the global spread of plastic regulations: An analysis of regulatory diffusion pathways through network analysis and visualization. *Korea and World Review*, 6(6), 987–1012. <https://doi.org/10.22743/kwr.2024.6.6.987>

Lee, H. Y., Kwon, B. G., & Cha, S. M. (2021). *Recent EU regulatory reforms concerning digital platforms and trade-friendly institutional improvement directions for Korea* (Long-Term Trade Strategy Study No. 21-01). Korea Institute for International Economic Policy. https://www.kiep.go.kr/gallery.es?act=view&bid=0001&list_no=9902&mid=a10101010000

Lee, K. I. (2024). The current status and challenges of regulatory discussions in Germany: Focusing on Germany's Network Enforcement Act (NetzDG) and the EU Digital Services Act (DSA). *Public Law Journal*, 25(2), 3–30. <https://doi.org/10.31779/plj.25.2.202405.001>

Lee, S. H., & Kim, H. (2022). Introduction and significance of the digital euro: Focusing on the European Digital Single Market and the EU's monetary sovereignty. *Journal of EU Studies*, 63, 247–272. <https://doi.org/10.18109/jeus.2022..63.247>

Lee, S. W. (2022). A study on China's algorithm governance: Focusing on the Provisions on the Administration of Algorithm Recommendations for Internet Information Services. *Northeast Asian Law Journal*, 16(1), 25–62.

Lee, S. Y. (2023). Current status and challenges of establishing norms related to artificial intelligence at home and abroad. *Korean Lawyers Association Journal*, 72(1), 442–488. <https://doi.org/10.17007/klaj.2023.72.1.014>

Linklaters. (2025, September 30). *Italy: A pioneering national framework to complement the EU AI Act*. <https://www.linklaters.com/en/insights/blogs/digilinks/2025/september/italy--a-pioneering-national-framework-to-complement-the-eu-ai-act>

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies*, 40(2), 235–258.

Martens, B. (2024). *The European Union AI Act: Premature or precocious regulation?* Bruegel. <https://www.bruegel.org/analysis/european-union-ai-act-premature-or-precocious-regulation>

Ministry of Science and ICT, Republic of Korea. (2020). *The Ministry of Science and ICT establishes human-centered artificial intelligence (AI) ethics standards*. <https://eiec.kdi.re.kr/policy/materialView.do?num=208784>

Ministry of Science and ICT, Republic of Korea. (2024). *Legal bases for fostering and regulating the artificial intelligence industry established: AI Basic Act passed by the National Assembly*. <https://www.korea.kr/news/policyNewsView.do?newsId=148937982>



Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity assessments and post-market monitoring: A guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, 32(2), 241–268. <https://doi.org/10.1007/s11023-021-09577-4>

Montagnani, M. L. (2019). *A new liability regime for illegal content in the Digital Single Market Strategy*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398160

National Law Review. (2025, November 18). *Italy enacts first national artificial intelligence law in EU*. <https://natlawreview.com/article/when-rome-make-your-ai-do-regulators-do>

Noh, M. H. (2023). The European Union's General Data Protection Regulation from the convergence perspective between the ripple effects of the Digital Single Market and the European tradition of human rights protection. *Historical Cultural Studies*, 85, 367–410. <https://doi.org/10.18347/hufshis.2023.85.367>

Oh, C. R. (2023). The Brussels Effect in the transition of international order: The hegemonic influence of the European Union's regulatory power. *Journal of EU Studies*, 65, 159–189. <https://doi.org/10.18109/jeus.2023..65.159>

Oh, T. H., & Kang, M. J. (2018). *The entry into force of the EU General Data Protection Regulation (GDPR): Evaluation and responses* (Today's World Economy No. 18-19). Korea Institute for International Economic Policy. https://www.kiep.kr/gallery.es?act=view&bid=0003&list_no=3389&mid=a10101010000

Park, J. H. (2024). National security-based restrictions on cross-border personal data transfer under digital economy agreements. *Korean Journal of International Law*, 69(4), 35–75. <https://doi.org/10.46406/kjil.2024.12.69.4.035>

Park, N. H., & Kim, H. K. (2024). A review of the EU Artificial Intelligence Act concerning personal data protection. *JURIS*, 1(68), 33–62. <https://doi.org/10.22825/juris.2024.1.68.002>

Rességuier, A., & Rodrigues, R. (2020). AI ethics should not remain toothless! A call to bring back the teeth of ethics. *Big Data & Society*, 7(2). <https://doi.org/10.1177/2053951720942541>

Shin, E. C., Kim, H. (2023). Digital Sovereignty and Europe: Legislation and Implications of EU Digital Policy. *Journal of EU Studies*, 67, 65–88. 10.18109/jeus.2023..67.65

Shim, S. Y. (2024). *The regulation-centered European Union Artificial Intelligence Act (EU AI Act)* (Latest Foreign Legislation Information No. 242). National Assembly Library. <https://nsp.nanet.go.kr/plan/subject/detail.do?nationalPlanControlNo=PLAN0000044995>

Walch, K. (2021, August 7). *Rigging for AI: How the US Navy embraces digital and masters AI with Brett Vaughan, Chief AI Officer and AI Portfolio Manager at the Office of Naval Research*. Forbes.



<https://www.forbes.com/sites/cognitiveworld/2021/08/07/rigging-for-ai-how-the-us-navy-embraces-digital-and-masters-ai/?sh=4c349d57abb3>

White & Case LLP. (2026, January 22). *AI Watch: Global regulatory tracker—Italy*. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-italy>

World Economic Forum. (2020). *Data Free Flow with Trust (DFFT): Paths towards free and trusted data flows*. <https://www.weforum.org/publications/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows/>

World Economic Forum. (2026). *The global risks report 2026* (21st ed.). <https://www.weforum.org/publications/global-risks-report-2026/>

Yang, C. S. (2024). The European Union Artificial Intelligence Act and AI regulation. *Regulatory Law Review*, 24(1), 127–172.

Yang, H. T. (2021). *Recent responses and implications of major countries for trustworthy artificial intelligence* (AI Trend Watch 2021-11). Korea Information Society Development Institute. <https://eiec.kdi.re.kr/policy/domesticView.do?ac=0000157467&issus=>

Yang, J. W. (2024). EU online platform regulation: Main contents and issues of the Digital Markets Act (DMA). *The Journal of Contemporary European Studies*, 42(1), 49–79. <https://doi.org/10.17052/jces.2024.42.1.49>

Yoon, J. H., & Cho, E. J. (2024). *Meaning and implications of the passage of the EU Artificial Intelligence Act (AI Act)* (Issue Brief No. 527). Institute for National Security Strategy.

https://www.inss.re.kr/publication/bbs/ib_view.do?bbsId=ib&nttId=41037112&page=1&searchCnd=0&searchWrd=