IE University IE International Policy Review (IPR)
Journal **7 Issue 1** (2026)
https://ipr.blogs.ie.edu/

Ethics AI and Fundamental Rights: A Comparative Analysis of EU and US Regulation

Gabriela Vázquez-Guillén

Law Department, IE University, Madrid, Spain.
Law and International Relations.

E-mail: gvazquezguil.ieu2023@student.ie.edu

Published January 2026

Editor: Will Thomas, Georgetown University

Abstract

This article examines the ethical and constitutional underpinnings of AI Governance in the US and EU. Discussing the roots of each jurisdiction's constitutional traditions, the article establishes the positive and negative conceptions of freedom present in each. The article examines how one conception of freedom manifests in legislative and legal texts with respect to AI regulation. The article details the unified, rights-focused approach of the EU, contrasting it with the more laissez-faire, disjointed approach of the US. The article examines early cases dealing with the use of AI in each jurisdiction, analyzing how their respective constitutional and ethical traditions influence case outcomes and legal approaches to AI regulation. The paper argues that, in furthering a more unitary approach to protecting fundamental rights such as dignity, the EU's approach is more likely to encourage a sustainable culture of responsible AI use.

Keywords: artificial intelligence, AI governance, fundamental rights, human dignity.

1. Introduction

It is undeniable that artificial intelligence (AI) has drastically impacted our lives. Its growing presence has become a defining force in global governance, forcing states to tackle the question of how to balance AI innovation with fundamental rights. Across the Atlantic, two distinct regulatory approaches have emerged. The European Union (EU) and the United States (US) have set their sights on disparate methods of AI regulation.

The EU has taken a rights-driven approach, focusing on safeguarding fundamental rights through regulations such as the AI Act. In contrast, the US has applied a market-driven approach. Adopting a more laissez-faire strategy, the US focuses on minimising state intervention and fostering innovation. With a plan focused on economic growth, the US has allowed companies to self-regulate.[1] The difference in their approaches is not coincidental, but rather stems from a long history of constitutional traditions. The EU's legal order is deeply rooted in the Charter of Fundamental Rights and the European Convention on Human Rights (ECHR), both

[1] Davtyan, Tatevik. 'The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained.' *Case Western Reserve Journal of Law, Technology & the Internet* 16, no. 2 (2025): 223. https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2.

of which focus heavily on positive constitutional rights. These rights identify activities that the government must perform, rather than dictating which infringements it cannot. However, the US enshrines a vision of negative constitutional rights, focusing on those activities the government must avoid. The EU adopts a more active stance toward AI governance, stepping in to protect citizens rights as a positive duty. The US, with the focus on what the government must not do, instead consigns AI regulation to the private sector for fear of overstepping.

This essay looks to analyze how the differing approaches to fundamental rights in the EU and the US shape their legal and ethical impacts on AI regulation. The European approach emphasizes human dignity and protection, while the American one focuses on individual liberty and limited government.

2.. Foundations of Fundamental Rights

1.1 The European Approach

The difference between the EU and the US with respect to AI regulation stems from their differences in constitutional traditions and the emphasis on certain fundamental rights. The European interpretation of fundamental rights is based largely on the principle of human dignity, impacting how rights such as privacy, equality, and data protection are interpreted and applied. This EU principle is enshrined in Article 1 of the European Union Charter of Human Rights, which ensures 'human dignity is inviolable. It must be respected and protected.'[2] The Charter calls for intervention in order to uphold fundamental rights in areas and cases where member states fall short.

One of the most important developments of the Charter is the recognition of a new fundamental right: the right to the protection of personal data. This right became the basis for the 2016 General Data Protection Regulation (GDPR). This constitutional approach to fundamental rights has had clear regulatory implications. This can be seen in Article 22 of the GDPR, which allows EU citizens 'the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her,'[3] reflecting the EU's protection of human rights by impeding a machine from making decisions which may undermine citizens' autonomy clearly protected by the GDPR.

The EU established clear limits on how personal data can be collected, processed, and shared, which ensures that citizens' privacy and dignity, is protected.Individuals are not viewed by the EU as mere consumers; they are instead rights-holders who deserve protection from abuse by big corporations, transparency, and accountability. This has consequently impacted the way AI is regulated in the EU, using a 'rights-driven framework, which focuses on safeguarding fundamental rights through comprehensive

[2] European Union, *Charter of Fundamental Rights of the European Union*, OJ C 364/1 (December 7, 2000), art. 1.
[3] European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, OJ L 119/1 (May 4, 2016), art. 22.

regulations."[4] In doing so, the EU ensures that technological innovation serves people, rather than the other way around.

3. The US Approach

The Bill of Rights, on the other hand, codifies the American conception of fundamental rights. These ten amendments were written to safeguard individual liberties and limit government power.[5] In *Katz v. United States* (1967), the Supreme Court held that a government's warrantless wiretapping of a public phone book violated the Fourth Amendment right to protection against unreasonable searches and seizures, demonstrating the negative-rights tradition present in the US.[6] In *Katz*, the right to privacy is considered largely defensive. The government is not obliged to take proactive steps to promote the privacy of its citizens, much less to refrain from restricting it.

The way AI has been regulated in the US has been influenced by this tradition, resulting in a policy framework that promotes innovation and self-regulation while limiting centralized oversight. The US approves sector-specific bills and advisory bodies rather than comprehensive regulation like the EU's GDPR or AI Act. The National Artificial Intelligence Initiative Act of 2020, which was passed as a component of the National Defence Authorisation Act, is a prime example. The National Artificial Intelligence Advisory Committee, which provided the president with advice on initiative-related issues, and an Artificial Intelligence Initiative were established by the act.[7] The Act directs federal agencies to fund research and support AI workforce development, but notably doesn't impose any binding rules on AI developers. Unlike the EU's GDPR Article 22, the United States lacks a federal right to human review of automated decisions. The US does not impose a duty on private actors to explain or justify algorithmic decisions. Rather than the unified, rights-based regulatory framework of the EU, this illustrates the US's longstanding dedication to innovation. As a result, it puts citizens' privacy at risk and puts innovation ahead of security.

The aforementioned framework reflects the US's focus on minimising regulatory intervention and guaranteeing innovation in the private sector. However, it's crucial to remember that some state and local laws can close this regulatory gap. Laws prohibiting discrimination through automated systems have been passed in Colorado, New York City, and Illinois. These generally allow consumers the right to opt out of data processing for profiling based on automated decisions that could result in legal effects on customers. These laws have also included policies on transparency, prior notice, and data protection.[8] While states are taking steps to regulate AI and protect citizens,

[4] Davtyan, 'U.S. Approach to AI Regulation,' 223.
[5] Bill of Rights Institute, 'Bill of Rights,' https://billofrightsinstitute.org/primary-sources/bill-of-rights.
[6] *Katz v. United States*, 389 U.S. 347 (1967).
[7] U.S. Congress, House, *National Artificial Intelligence Commission Act*, H.R. 6216, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/6216.
[8] White & Case LLP, 'Automated Decision-Making Emerges as an Early Target in State AI Regulation,' *White & Case Insights*, July 9, 2024, https://www.whitecase.com/insight-alert/automated-decision-making-emerges-early-target-state-ai-regulation.

these are driven by a more state-level constitutional tradition.[9]

4. Legal and Ethical Frameworks for AI Regulation

4.1 The EU Model

Using human dignity and fundamental rights as its basis, the European Union has played a major role in developing a comprehensive legal and ethical framework for AI regulation: the AI Act (Regulation (EU) 2024/1689) in August 2024. The act will come fully into force in August 2026.[10] The AI Act takes a risk-based approach, categorizing applications into four risk levels: unacceptable, high, limited, and minimal.[11] Each one is subject to different legal obligations. For example, high-risk AI systems such as 'social scoring systems and manipulative AI'[12] may be subject to risk assessments and mitigation measures. In contrast, those AI platforms with minimal or no risks, such as 'AI-enabled video games,'[13] will be subject to minimal regulation. This act sets a clear set of rules for AI developers, in an effort to ensure 'that Europeans can trust what AI has to offer.'[14]

However, this is not the only legislation that regulates AI; the GDPR also safeguards personal data. Its principles of lawfulness and transparency extend to AI systems, which often rely on large-scale processing of personal data. For example, under the GDPR's Article 6, a developer can't gather personal images or social media content to train an AI model unless there is a lawful basis for such.[15] This was illustrated in the Clearview AI case, in which France fined the company for violating Article 6, due to the processing of EU residents' photos for facial recognition training, which constituted an unlawful use of processing.[16] Additionally, the EU has a set of ethical guidelines and digital regulations that collaborate to ensure 'that AI is developed in a manner that is safe, transparent, and respectful of fundamental rights.'[17]

The creation of trustworthy AI ensures that technological innovation does not undermine citizens' rights by proactively limiting the transgressive powers of AI

[9] Hershkoff, Helen. "Positive Rights and State Constitutions: The Limits of Federal Rationality Review." *Harvard Law Review* 112, no. 6 (1999): 1131–96. https://doi.org/10.2307/1342383.

[10] European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (AI Act)*, OJ L 202/1 (July 12, 2024), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[11] Sofia Gracias, 'Artificial Intelligence and Regulation: A Comparative Analysis of the EU and U.S. Approaches,' *University of Chicago Business Law Review* 4, no. 1 (2024): 1, https://businesslawreview.uchicago.edu/sites/default/files/2024-03/Sofia%20Gracias.pdf.

[12] ArtificialIntelligenceAct.eu, 'High-Level Summary of the EU AI Act,' https://artificialintelligenceact.eu/high-level-summary/.

[13] Ibid.

[14] European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (AI Act)*, OJ L 202/1 (July 12, 2024), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[15] European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, OJ L 119/1 (May 4, 2016), art. 6.

[16] European Data Protection Board, 'French SA Fines Clearview AI EUR 20 Million,' news release, October 21, 2022, https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

[17] Itziar López de Maturana y de Uriarte, 'Artificial Intelligence, Human Rights and Business Responsibilities,' *Deusto Journal of Human Rights* 8, no. 2 (2021): 43–70, https://djhr.revistas.deusto.es/article/view/3263/4184.

systems and the companies that create them. Additionally, the EU has established a timeline for AI developers. By not coming into effect until 2026, the gap between approval and implementation of the act shows a balance between rights and privacy protection with AI innovation. The EU has shown a willingness to work around the needs of AI developers, even as it remains uncompromising in the eventual implementation of a rights-first approach.

Through the prohibition of AI practices that may violate human dignity and blocking platforms which pose an unacceptable risk, the EU ensures its citizens are free from government overreach and from corporate malfeasance. However, some may argue that the risk-based approach could lead to overregulation, stifling innovation, and harming industry growth.[18] However, these concerns aren't as crucial as protecting privacy and the safety of citizens.

4.2 The US Model

While the EU has very clear AI regulations, the U.S. lacks a comprehensive federal law that specifically governs its use and implementation. The US approach to regulating AI is more decentralized than the EU's. The focus on protecting individual liberties and limited government interference, as enshrined in the Bill of Rights, creates a legal culture in which protection from government violations is the first priority. That said, the US has various legislative, executive, and agency-based initiatives, albeit disjointed.

While members of Congress have introduced hundreds of bills in relation to artificial intelligence, fewer than 30 have been enacted since May of 2025.[19] Many of the proposed bills have 'emphasized the development of voluntary guidelines and best practices and reporting of industry-conducted evaluations of AI systems rather than prohibitions or independent evaluation of AI uses and technologies.'[20] This clearly reflects a commitment to private self-regulation and stimulating innovation.

Similarly, the Bipartisan Framework by Senators Blumenthal and Hawley demonstrates an emphasis on consumer protection, transparency, and national security.[21] The framework includes licensing for high-risk AI companies, ensuring legal accountability, promoting transparency, and defending national security. The focus on accountability mechanisms shows the US's fragmented approach, rather than the use of a unified legislative act.

The United States's AI governance framework embodies those fundamental principles clearly stated in the Bill of Rights. While the US demonstrates a need for regulation and safeguards, it prioritizes innovation through minimal state intervention. This is consistent with the

[18] Sofia Gracias, 'Artificial Intelligence and Regulation: A Comparative Analysis of the EU and U.S. Approaches,' *University of Chicago Business Law Review* 4, no. 1 (2024): 1, https://businesslawreview.uchicago.edu/sites/default/files/2024-03/Sofia%20Gracias.pdf.

[19] Congressional Research Service, *Artificial Intelligence: Overview, Recent Developments, and Issues for Congress*, CRS Report R48555 (Washington, DC: Library of Congress, 2023), https://www.congress.gov/crs_external_products/R/PDF/R48555/R48555.2.pdf.

[20] Ibid.

[21] Ibid.

belief that centralized control stifles progress, and individual freedom and market competition ensure it. However, the lack of specific, unified protections for citizens is of greater concern than innovation. In failing to produce these, the US framework has failed compared to the EU framework.

5. Comparison between the two models and Policy Recommendations

The European Union and the United States approach AI regulation differently, which is rooted in their differing legal and philosophical traditions. The EU 'applies uniformly across all AI systems and sectors, establishing a comprehensive, cross-sector regulatory framework', whereas the US 'adopts a decentralized, sector-specific strategy.'[22] The EU's precautionary framework embodies Article 1 of the EU Charter of Fundamental Rights and its commitment to protecting human dignity and individual rights.[23] The US's market-driven and sector-fragmented framework demonstrates the application of constitutional principles of individual liberty and limited government. Additionally, while the EU applies its legislation to all Member States, thereby directly affecting the private sector, the US fails to protect its citizens from private abuses.

Both systems recognize the need for trustworthy AI and incorporate risk-based approaches; however, their constitutional traditions cause them to diverge on the questions of methods and degree. The EU follows a proactive, positive rights-based approach to ensure fundamental rights, whereas the US follows a more reactive, negative rights-based approach to emphasize competition and innovation. Therefore, the EU more effectively protected fundamental rights, which, after all, is the priority.

5.1: Case Law Practical Applications

5.1.1: EU

In the European Union, case law illustrates how fundamental rights shape the limits placed on emerging technologies such as *AI. In Case C-634/21 (SCHUFA)*, the CJEU held that algorithmic credit-scoring constitutes a decision 'based solely on automated processing.'[24] Under Article 22, 'The data subject shall have the right not to be subject to a decision based solely on automated processing.'[25] Therefore, this case demonstrated that algorithmic credit-scoring lacked transparency regarding the logic involved and presented various risks to human dignity. Similarly, in Case C-184/20, which concerned Lithuania's publication of officials' financial decorations, the Court found that large-scale disclosure of personal data was in violation of the GDPR principles of data minimization and necessity. The publication of such extensive information made individuals easily identifiable and violated their privacy, demonstrating the

[22] Davtyan, Tatevik. 'The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained.' *Case Western Reserve Journal of Law, Technology & the Internet* 16, no. 2 (2025): 223. https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2.

[23] European Union, *Charter of Fundamental Rights of the European Union*, OJ C 364/1 (December 7, 2000), art. 1.

[24] European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, OJ L 119/1 (May 4, 2016), art. 22.

[25] Ibid.

proportionality and strict control the EU enforces when it comes to data protection. Both of these cases show how the EU respects fundamental rights and restricts AI systems that may abuse these.

Therefore, the EU should keep strengthening its rights-based approach to AI governance, making sure current laws are effectively enforced. To avoid regulatory fragmentation, special attention should be given to bolstering supervisory capacity and standardizing enforcement among Member States. The EU should make clear its obligations regarding transparency, human oversight, and proportionality as the AI Act comes into effect, particularly for high-risk AI systems used by private actors. Furthermore, mechanisms for continuous assessment should be put in place to determine whether risk classifications are still appropriate as technology advances. The EU can sustain innovation while upholding its fundamental commitment to human dignity and rights by combining strict enforcement with flexible regulatory review.

5.1.2: US

U.S case law represents the country's negative-rights constitutional structure and its corresponding permissive approach to private AI development. In the Meta Platforms, *Inc. v. Bright Data Ltd.*, in which Meta sued Bright Data, a scraping company for extracting Facebook and Instagram data used in AI-related applications. Because the US lacks a federal privacy or AI statute restricting the large-scale collection of personal data, Meta had to fight the case through its Terms of Service, relying on contract and competition law, not through a rights-based framework. The court rejected Meta's argument that Bright Data's actions were a breach of contract because the scraping occurred while users were logged out, meaning they weren't bound by the contract obligations that applied to logged-in users.[26] This underscores the larger issue: Meta was forced to depend on inadequate legal tools which were never designed to protect privacy. This clearly represents how the US' negative-rights approach leaves citizens exposed to the risks of AI abuse.

In order to mitigate the increasing risks associated with AI systems, especially those that impact privacy, equality, and autonomy, the United States should implement basic federal protections. A restricted rights-based framework that emphasizes accountability, transparency, and human oversight would lessen the need for contract and competition law, which are ill-suited to deal with systemic AI harms. Individual protections would be greatly strengthened without compromising innovation if a federal right to meaningful human review of high-impact automated decisions were established. In order to ensure that private AI development does not undermine fundamental rights, such reforms would address the regulatory gaps revealed by recent case law while maintaining the US commitment to minimal government intervention.

6. Conclusion

[26] *Meta Platforms, Inc. v. Bright Data Ltd.*, No. 3:23-cv-00077 (N.D. Cal.), doc. 145, filed February 12, 2024, https://docs.justia.com/cases/federal/district-courts/california/candce/3:2023cv00077/406956/145.

The divergent approaches of the EU and the US to AI regulation don't just reflect policy preferences, but deeply embedded constitutional traditions. The EU's legal order is grounded in human dignity and positive rights, placing obligations on governments and private actors to safeguard privacy and transparency. These are manifested in and driven by the GDPR and AI Act. The current CJEU case law has also reinforced the use of this framework. By prioritizing fundamental rights in the development of technology, the EU seeks to ensure that AI development occurs while ensuring that individuals and democratic values are upheld. As a result, the EU has been far more successful in embedding fundamental rights into AI regulation than the US.

In contrast, the United States relies on negative rights and limited government, focusing on a decentralized, innovation-first environment. Federal oversight is sectoral, leaving private companies broad discretion to self-regulate, and prioritizing innovation, which also leaves the door wide open for private abuses. While both systems recognize the fast-growing rate of AI and the need for transparent and trustworthy technology, the EU's proactive, positive constitutional tradition enables greater protection of its citizens from private abuse, and therefore is a more sustainable effort to balance innovation with human dignity.

Bibliography

Table of Cases

Katz v. United States, 389 U.S. 347 (1967).

Meta Platforms, Inc. v. Bright Data Ltd., No. 3:23-cv-00077 (N.D. Cal.), doc. 145, filed February 12, 2024, https://docs.justia.com/cases/federal/district-courts/california/candce/3:2023cv00077/406956/145.

Table of Legislation

European Union, *Charter of Fundamental Rights of the European Union*, OJ C 364/1 (December 7, 2000), art. 1.

European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, OJ L 119/1 (May 4, 2016), art. 22.

European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (AI Act)*, OJ L 202/1 (July 12, 2024), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

U.S. Congress, House, *National Artificial Intelligence Commission Act*, H.R. 6216, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/6216.

List of References

ArtificialIntelligenceAct.eu, 'High-Level Summary of the EU AI Act,' https://artificialintelligenceact.eu/high-level-summary/.

Bill of Rights Institute, 'Bill of Rights,' https://billofrightsinstitute.org/primary-sources/bill-of-rights.

Congressional Research Service, *Artificial Intelligence: Overview, Recent Developments, and Issues for Congress*, CRS Report R48555 (Washington, DC: Library of Congress, 2023), https://www.congress.gov/crs_external_products/R/PDF/R48555/R48555.2.pdf.

Davtyan, Tatevik. 'The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained.' *Case Western Reserve Journal of Law, Technology & the Internet* 16, no. 2 (2025): 223. https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2.

European Data Protection Board, 'French SA Fines Clearview AI EUR 20 Million' (Press Release, 21 October 2022)

Itziar López de Maturana y de Uriarte, 'Artificial Intelligence, Human Rights and Business Responsibilities,' *Deusto Journal of Human Rights* 8, no. 2 (2021): 43–70, https://djhr.revistas.deusto.es/article/view/3263/4184.

Sofia Gracias, 'Artificial Intelligence and Regulation: A Comparative Analysis of the EU and U.S. Approaches,' *University of Chicago Business Law Review* 4, no. 1 (2024): 1, https://businesslawreview.uchicago.edu/sites/default/files/2024-03/Sofia%20Gracias.pdf.

Hershkoff, Helen. "Positive Rights and State Constitutions: The Limits of Federal Rationality Review." *Harvard Law Review* 112, no. 6 (1999): 1131–96. https://doi.org/10.2307/1342383.

White & Case LLP, 'Automated Decision-Making Emerges as an Early Target in State AI Regulation,' *White & Case Insights*, July 9, 2024, https://www.whitecase.com/insight-alert/automated-decision-making-emerges-early-target-state-ai-regulation.