South American Publishing

SAP Social AI. 2025; 1:51
doi: 10.62486/sai202551

REVIEW

Analysis of global trends in reference frameworks associated with artificial intelligence

Análisis de las tendencias globales en marcos de referencia asociados a la inteligencia artificial

Lawrence Rodrigo Loaiza Solano[1], Luis Diego Moya Rojas[1], Sebastián Alejandro López Luna[1]

[1]Universidad Latinoamericana de Ciencia y Tecnología, Ingeniería Informática. San José, Costa Rica.

Cite as
Loaiza Solano LR, Moya Rojas LD, López Luna SA. Analysis of global trends in reference frameworks associated with artificial intelligence. SAP Social AI. 2025; 1:51. https://doi.org/10.62486/sai202551

Publication History
Submitted: 13-06-2025
Revised: 24-08-2025
Accepted: 16-10-2025
Published: 17-10-2025

Corresponding Author
Lawrence Rodrigo Loaiza Solano

ABSTRACT

This article analyzed global trends in AI reference and regulatory frameworks in the EU, the United States, and China based on an integrative literature review (2020–2025). It identified convergences in values such as transparency, fairness, and accountability, but major divergences in implementation. The EU advanced a binding, risk-based model; the U.S. maintained voluntary guidelines that prioritize innovation; and China adopted a centralized approach centered on security and content control. Cases like Clearview AI and Apple Card illustrated risks of bias and data misuse, reinforcing the need for stronger governance. The study concluded that limited global harmonization hinders interoperability and called for minimum standards, multilateral oversight, and clearer guidance for generative AI.

Keywords: Artificial Intelligence Regulation; Data Protection; Interim Measures for AI Regulation; United States; European Union; China.

RESUMEN

Este artículo analizó comparativamente las tendencias globales en los marcos de referencia y regulación de la IA en la Unión Europea, Estados Unidos y China, a partir de una revisión bibliográfica entre 2020 y 2025. Identificó coincidencias en valores como transparencia, equidad y rendición de cuentas, pero claras diferencias en su aplicación. La UE avanzó con un modelo vinculante basado en niveles de riesgo; EE. UU. mantuvo lineamientos voluntarios orientados a la innovación; y China adoptó un enfoque centralizado centrado en la seguridad y el control informativo. Casos como Clearview AI y Apple Card mostraron riesgos de sesgo y uso indebido de datos. El estudio concluyó que la falta de armonización global limita la interoperabilidad y destacó la necesidad de estándares mínimos, supervisión multilateral y lineamientos para la IA generativa.

Palabras clave: Regulación de la Inteligencia Artificial; Protección de Datos; Medidas Provisionales para la Regulación de la IA; Estados Unidos; Unión Europea; China.

© 2025; The Authors. This Open access article is distributed under the Creative Commons Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

AI governance frameworks bring together norms and procedures that guide automated systems and incorporate privacy laws such as the GDPR, CCPA, and LGPD as data-processing obligations shape system accountability.[1,4] As the scale and capability of AI increase, privacy and transparency risks increase, making regulatory instruments essential for balancing benefits and societal harm.[3,5] Studies highlight the disconnect between ethical principles and binding rules, stressing the need for operational standards tailored to national and sectoral contexts.[4,6] Despite global guidance, effective enforcement remains regional, as seen in the EU AI Act or the U.S. and China's sector-based approaches.[2,6,7] The U.S., the EU, and China were selected for comparison because of their central influence: the U.S. leads in R&D and applies largely voluntary frameworks.[8,9] The EU advances an extraterritorial model through the AI Act.[8] Finally, China is rapidly institutionalizing regulations, especially for generative AI.[10] Together——these jurisdictions illustrate the key technological and regulatory trends shaping global AI governance.

Objective and Scope

This study conducts a comparative analysis of major AI regulatory frameworks, including the EU AI Act, the U.S. Blueprint for an AI Bill of Rights, and China's rules on algorithms and generative models.[11,12] It identifies key convergences, divergences, and regulatory gaps relevant to future international governance aimed at ethical and safe AI development.[11] The analysis covers ethical-legal principles, transparency, and fundamental rights.[13] Regional policies for managing AI risk.[4] It also reviews prevailing enforcement and oversight mechanisms to mitigate societal impacts.[14] In addition, it assesses the coherence of these frameworks with broader standards such as UNESCO's principles.[13]

Justification

AI governance remains fragmented because of the absence of a binding global framework. UNESCO's ethical recommendation lacks enforceability.[13] The EU's AI Act introduces risk-based obligations regarding transparency and human oversight.[14,15] The United States relies on decentralized, voluntary principles such as the Blueprint for an AI Bill of Rights and the NIST AI RMF.[16,17] China applies an interventionist model focused on national security and information control.[18] These divergences complicate global harmonization and allow firms to operate within permissive jurisdictions.[4]

Illustrative cases—such as Clearview AI's unlawful collection of facial data.[19] The gender-biased credit limits of the Apple Card algorithm.[20] These examples highlight concrete risks, supporting calls for a balanced global framework that protects rights while enabling innovation.[14,21,22] Recent sanctions against Apple Card and Clearview AI under the GDPR further demonstrate the real and measurable harms posed by AI.[23,24] This context underscores the need for harmonized standards and effective oversight bodies to safeguard data protection, accountability, and legal responsibility in AI deployment.[25]

Literature Review

AI governance encompasses the policies, technical mechanisms, and ethical–legal principles that guide the design and use of artificial intelligence, promoting fairness, transparency, safety, and accountability.[14] In the European Union, the AI Act applies a risk-based approach and prohibits practices such as biometric categorization without consent.[15,26] In the United States, the Blueprint for an AI Bill of Rights and the NIST AI RMF promote nonbinding ethical governance.[16,17] China has adopted strict regulations on algorithms and generative systems, requiring registration and information controls.[18]

Key principles of AI governance include algorithmic transparency, understood as the ability to audit and explain automated decisions.[26,27] Responsibility and traceability are also essential, allowing the identification of the origin and justification of outputs.[28] Human oversight remains crucial for supervising critical processes and preventing full delegation to autonomous systems.[16] Together, these components show that governance goes beyond drafting laws and requires international cooperation to balance innovation with rights protection amid global fragmentation.[13]

The deployment and use of AI have grown rapidly since 2022, driven by the use of generative tools and their integration into multiple sectors. According to the University of Melbourne and KPMG, two-thirds of people use AI regularly, 58 % of workers use it frequently, and 83 % of students apply it weekly or daily in academic settings.[29] Additionally, 75 % of organizations report adopting AI across multiple functions, and nearly half indicate that it generates revenue, indicating systemic incorporation.[29]

Compared with advanced economies, emerging economies show higher levels of use, training, and perceived effectiveness: 80 % vs. 58 % for regular use, 50 % vs. 32 % for training, and 74 % vs. 51 % for effectiveness. This rapid expansion exceeds institutional capacity to provide adequate governance and training.[29] The report also highlights risky behaviors—such as uploading sensitive information to public tools with or accepting results without critical analysis—which pose urgent challenges regarding privacy, security, and the regulation of AI use.[29]

AI faces issues such as dataset and model bias that lead to discrimination in hiring, the justice system, and facial recognition while also enabling expanded surveillance and mass data collection.[30] Additional risks, including cyberattacks, malicious use, and system failures, are exacerbated by black-box opacity, which complicates traceability and accountability.[31] Shams et al. highlight these challenges: of 551 incidents in AIID, 189 (34,3 %) are related to diversity and inclusion; in AIAAIC, 144 of 310 (46,45 %) fall under the same category.[32]

Beyond these incidents, more complex cases demonstrate inappropriate or harmful uses of AI affecting thousands or millions of users.

Clearview AI, a U.S. facial recognition company, collected billions of publicly available images to construct a biometric database and train its model, violating principles of consent, transparency, purpose limitations, and data minimization. This led to investigations

and significant penalties.[24] Under the GDPR, France fined the company €20 million (plus €5,2 million for noncompliance), while Italy and Greece each imposed additional €20 million fines.[24]

Two other widely known cases illustrate similar concerns:

- Spotify's Equalizer Project adjusted recommendations to increase the visibility of female artists, using algorithmic metrics to correct historical underrepresentation and sparking debate over proactive interventions.[23]
- Apple Card/Goldman Sachs faced claims that women received lower credit limits than men with similar profiles did, triggering investigations and demands for model transparency. Although intentional discrimination was denied, the case increased pressure for audits and explainability in automated financial decisions.[23]

The EU's GDPR protects privacy through seven principles in Article 5: lawfulness, fairness and transparency, purpose limitations, data minimization, accuracy, storage limitations, integrity/confidentiality, and accountability.[33] Article 4 defines three parties involved in processing, and Article 83 grants sanctioning powers to supervisory authorities.[34] Although not created specifically for AI, it restricts AI use involving personal data, preventing mass surveillance, opaque decisions, and automated bias.[35] Complementarily, the EU AI Act regulates autonomous or adaptive systems through risk levels (from unacceptable to high) and imposes strict requirements before deployment.[36]

In the United States, a flexible, innovation-oriented approach prevails, allowing for state-level laws because of the absence of a comprehensive federal framework.[37] The NIST AI RMF provides voluntary risk-management guidance through GOVERN, MAP, MEASURE, and MANAGE.[38] Its sociotechnical foundation promotes best practices and maturity models applicable across AI systems.[39] In data protection, the CCPA strengthens consumer rights but resembles the GDPR only in its application to large firms operating in California.[40]

In China, the Personal Information Protection Law (PIPL, 2021) safeguards personal data similarly to the GDPR, granting rights to access, rectify, erase, and port data, as well as to request explanations for automated decisions while requiring consent and transparency.[41,42] The Interim Administrative Measures for Generative AI Services (2023) regulate public generative AI through labeling requirements, training-data controls, correction mechanisms, and security assessments—balancing innovation with information security, differing from the EU's risk-based model.[43]

Although the EU, U.S., and China all apply risk-based approaches, implementation varies. The EU defines clear tiers—from unacceptable to minimal—while the U.S. NIST RMF provides contextual risk guidance without fixed categories.[21] China evaluates risks on the basis of "public interests" and "national security," requiring strict security reviews in critical sectors.[22]

Key differences also emerge in ethical principles, bias mitigation, and regulatory scope:

- The EU prioritizes fundamental rights; aligns the AI Act with the GDPR; and emphasizes data minimization, consent, and individual rights.[21] The US's NIST RMF promotes reliability, security, accountability, transparency, and equity, encouraging "privacy-enhanced" systems, although federal data protection is fragmented.[23] China applies principles of equity and privacy, but the PIPL operates under strict state supervision and data localization requirements.[23,24]
- All three seek transparency and bias mitigation. The EU imposes strict requirements (explainability) for high-risk AI and bans discriminatory practices such as "social scoring" (China).[21] The US promotes these through voluntary guidelines.[23] China mandates transparency in recommendation algorithms and content labeling and prohibits discrimination.[23,24] In terms of accountability, the EU defines clear responsibilities, the US encourages auditability, and China mandates shared responsibility (registration/audit).[25,24]
- Enforcement is centralized with significant penalties in the EU and China, whereas the US relies on voluntary organizational adoption and sector-specific norms.[21,25] The EU seeks a global standard with an extraterritorial effect (Brussels effect). The U.S. promotes international cooperation through voluntary frameworks, while China prioritizes technological sovereignty.[21,23,24,25]

Finally, the evaluation by KPMG and the University of Melbourne identifies structural deficiencies in global AI governance. Despite the abundance of principles, most are aspirational and lack binding mechanisms or uniform procedures.[5] This creates a gap between ethics and practice, leading to inconsistent responsibilities and limited accountability pathways.[5] Fragmentation across jurisdictions increases compliance burdens, enables regulatory arbitrage, and results in uneven protection of rights.[5] No binding global mechanism currently harmonizes principles or defines minimum standards; thus, AI governance remains largely national or regional, without treaty-level coordination for coherent global oversight and remediation.[5]

METHOD

Type of study

An integrative bibliographic review was conducted using secondary sources, as this approach is among the most effective ways to initiate a study by identifying similarities and differences across referenced articles.

Databases used

Google Scholar, ResearchGate, ACM Digital Library, Springer Nature Link, SSRN, SpringerOpen, and arXiv.org.

Search terms

"AI regulation in the US," "AI regulation in China," "AI regulation in the EU," "data privacy in China," "data privacy in

California."

Search period: 2020–2025.

Language criteria: English-language documents.

Inclusion criteria

Articles addressing AI regulatory frameworks in the EU, U.S., or China, as well as articles on data privacy or data protection laws linked to those AI regulatory systems.

Exclusion criteria

Articles focused on frameworks, laws, or standards not specifically tied to AI regulation (e.g., cybersecurity, software algorithms).

Analysis process

A two-phase search strategy was applied:

- Phase 1: Search terms and Boolean operators were used across the databases to identify documents by title and abstract. The results were exported, and duplicates were removed.
- Phase 2: Preselected articles were reviewed in full to verify compliance with the inclusion criteria.

From the final set of articles, the following elements were extracted:

a) the primary regulatory approach,
b) mandatory or recommended ethical principles, and
c) The proposed governance or compliance mechanisms in each region.

To support comparative analysis, all extracted information was organized by region—the European Union, the United States, and China—to identify similarities, differences, and cross-regional trends.

RESULTS

Table 1. Comparative Matrix between the NIST AI RMF, the EU AI Act, and China's Interim Administrative Measures for Generative AI

Characteristic	EU AI Act (European Union)	NIST RMF (U.S.)	Interim Measures (China)
General Approach	Binding, rights-based, with a harmonized risk hierarchy.	Voluntary, flexible, risk-based, promoting innovation.	State-driven, security-focused, emphasizing national control and stability.
Risk Classification	Four risk levels—Unacceptable, High, Limited, Minimal.	Adaptive; organizations set their own risk tolerance.	Based on social impact and national security, with strict reviews in critical sectors.
Key Ethical Principles	Human-centricity, protection of rights, transparency, oversight, accountability.	Reliability, safety, explainability, privacy, fairness.	Social harmony, controllability, political security, state-bounded privacy.
Transparency and Explainability	Mandatory for high-risk systems, including disclosure of AI interaction and deepfake labeling.	Voluntary, user-tailored disclosures.	Required transparency for recommendation algorithms and AI-generated content.
Privacy and Data	GDPR-compliant; strong rights and data minimization.	Technical privacy-enhancing measures.	Data protection subordinated to national security and localization.
Bias and Discrimination	Prohibits discriminatory uses; requires mitigation.	Treated as reliability issues.	Bans discriminatory recommendations; promotes social fairness.
Accountability and Enforcement	Legal liability with mandatory documentation and compliance.	Traceability through internal audits.	State-driven auditability for regulatory inspection.
Enforcement and Oversight	Centralized supervision by the EU AI Office with significant financial penalties.	Decentralized oversight relying on market adoption and existing sectoral agencies (e.g., FTC, FDA).	Strong state-led supervision by the Cyberspace Administration (CAC) with severe administrative sanctions.
Global Considerations	Extraterritorial global standard-setting.	International alignment through voluntary frameworks.	Global influence with a focus on technological sovereignty.

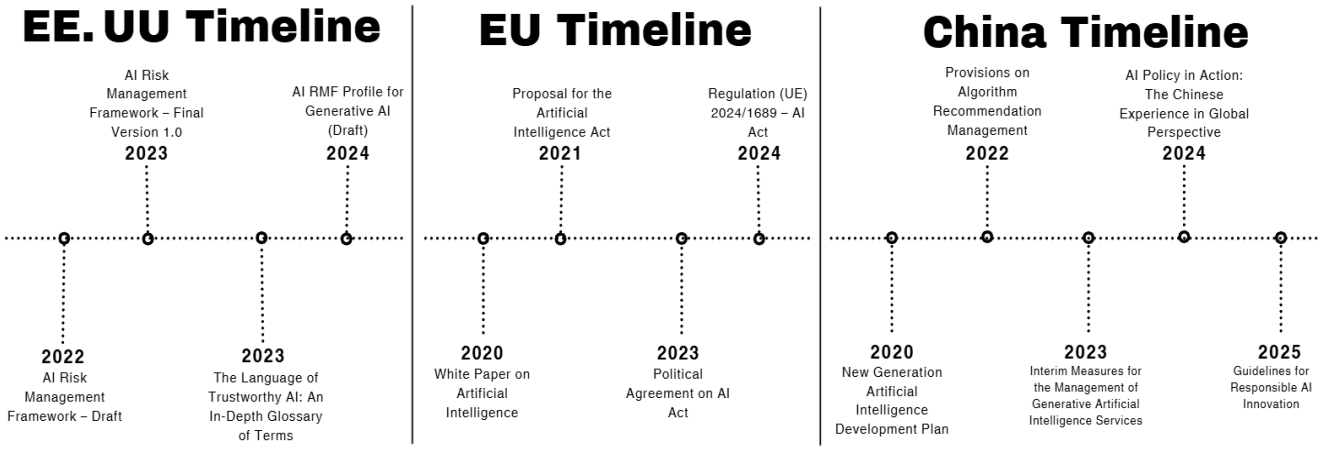


Figure 1. Timelines by reference frames

NIST provides a structured, trustworthy AI framework that evolved from draft to the final AI RMF 1.0, reinforcing transparency, security, and explainability.[17,44] The framework helps organizations identify, assess, and mitigate risks, strengthening confidence across the public and private sectors.[17] The Language of Trustworthy AI supports shared understanding through a standardized glossary.[45] The Generative AI Profile (Draft) extends guidance to risks in automated content creation and information manipulation.[26]

The EU has made progress toward harmonized AI rules. As shown in Figure #1, the framework evolved from the white paper on artificial intelligence, promoting "trustworthy AI" and innovation alongside rights protection and safety.[46] The AI Act introduced a risk-based regulatory model.[47] A political agreement emphasized transparency, explainability, and human oversight.[48] The adoption of Regulation (EU) 2024/1689 solidified the EU's ethical and responsible AI governance.[49]

China has developed a centralized and strategic AI regulatory framework, as shown in Figure #1, on the basis of the New Generation Artificial Intelligence Development Plan, which prioritizes security, economic growth, and social governance.[50] The Provisions on Algorithm Recommendation Management mandate transparency, data regulation, and content moderation.[18] The interim measures for generative AI services focus on safety, content control, and licensing.[51] Additional guidelines promote responsible innovation and reinforce China's international regulatory model.[52,53]

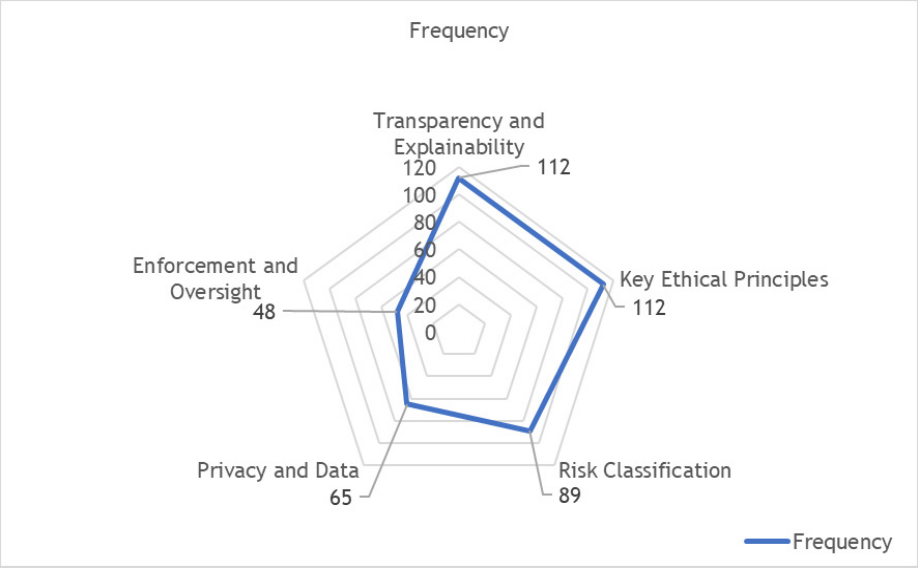


Figure 2. The five factors with the highest frequency across the analyzed articles

The five most frequently discussed governance factors across the reviewed literature are as follows: Transparency and Explainability (112 mentions) and Key Ethical Principles (112 mentions) dominate the discourse, reflecting the emphasis of global ethics guidelines and foundational ethical frameworks;[4,5,11,13] the prominence of Risk Classification (89 mentions) aligns with the EU's risk-based AI Act; and the risk-management orientation of the NIST RMF[1,15,17] Privacy and Data (65 mentions) mirror GDPR-style data-protection regimes and OECD concerns about data governance[1,6,33] and Enforcement and Oversight (48 mentions) corresponds to strong administrative enforcement models in the EU and China and to high-profile enforcement cases such as Clearview AI (figure 2).[10,15,19]

DISCUSSION

Regulatory Models: U.S., the EU, and China

United States: Voluntary and Functional Approach

The U.S. model, articulated through NIST's AI RMF, is voluntary and relies on technical guidance and organizational responsibility.[17,26] From early drafts to the generative AI profile, the process emphasizes trust and transparency.[17,26,38,39] This evolution balances innovation with responsibility, avoiding strict legal obligations.[41,48]

European Union: Binding Framework and Rights

The EU progressed from conceptual debates to the AI Act, establishing a harmonized and binding framework.[15,22] It incorporates risk-based classification, transparency, and human oversight to reinforce rights protection and accountability.[15,22,31,33] The "Brussels effect" promotes global ethical standards.[20,23]

China: National Security and State Control

China embeds AI in national security planning. Measures for generative AI combine technological innovation with strict content oversight.[18,32] Requirements such as algorithm registration and licensing are designed to expand state authority and digital sovereignty.[43,52,53] Additionally, AI development is linked to social stability and technological power.[28]

Convergences and Divergences in Application

Transparency and explainability are shared principles but are applied differently. The EU enforces formal requirements such as technical documentation, which increases compliance but places a burden on SMEs. The U.S. relies on voluntary frameworks and sector-specific rules, resulting in uneven protection.[54] China emphasizes security, requiring internal audits and reporting obligations for public disclosure.[54]

Risk management also differs. The EU employs a strict regulatory hierarchy with explicit prohibitions.[55] The U.S., through NIST, adopts flexible management functions.[17,55] China evaluates the impacts on public interests and national security.[55] These conceptual differences hinder the definition of "high-risk" systems globally and complicate audit harmonization.[56]

The enhancement capacity varies significantly. The EU and China use strong administrative mechanisms involving fines and oversight.[17] Europe's coercive authority supports effective enforcement, as demonstrated in the Clearview case.[23] The U.S. lacks a federal punitive system, relying instead on agencies such as the FTC and FDA, which creates inconsistencies.[17,57] China is rapidly institutionalizing supervision to preserve public order.[58]

CONCLUSIONS

The review reveals a core paradox: while there is broad consensus on protected values such as transparency and fairness, the ways in which they are implemented diverge sharply. The EU, U.S., and China act as architects of the global AI regime, yet their distinct compliance paths hinder legal and technical interoperability, making cross-border certification or mutual recognition extremely difficult and costly. The U.S. prioritizes voluntary, innovation-oriented frameworks, whereas the EU adopts prescriptive rules that safeguard rights but burden startups. China focuses on controlling corporate autonomy and shaping industrial structure and SME competitiveness. The policy challenge is to craft verifiable, cross-jurisdictionally compatible rules through shared risk metrics, minimum traceability standards, and multilateral enforcement cooperation.

For future work, empirical measures should be considered to assess the actual effectiveness of the legal frameworks analyzed, particularly through longitudinal databases of sanctions, audits, and administrative rulings. It is essential to examine how compliance costs vary across regions and their impacts and to expand the analysis to emerging economies and relevant stakeholders. Finally, an international taxonomy of "high risk" should be developed, and the rapidly evolving regulations for generative AI, including technical challenges, traceability, and content control, should be examined in a global context.

RECOMMENDATIONS

Advancing responsible and coherent AI governance requires hybrid regulatory models that combine binding obligations for high-risk systems with flexible guidance to preserve innovation. This includes defining clear risk categories, shared thresholds, and robust traceability supported by technical documentation, impact assessments, and records enabling independent, reproducible audits. Cross-border coordination should be strengthened through information sharing, joint supervisory protocols, and limited mutual recognition of certifications. Interoperable technical standards—common formats, metrics, and evaluation methods—would ease compliance across jurisdictions. International guidelines for generative AI should also address transparency, labeling, and content governance. Organizations need accessible compliance tools such as practical guidelines, templates, and training to reinforce institutional capacity. Public participation should be promoted through reporting channels and redress mechanisms that enhance trust in responsible AI deployment.

FUNDING

The authors did not receive funding for the development of this research.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Data curation: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Formal analysis: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Research: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Methodology: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Project management: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Resources: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Software: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Supervision: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Validation: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Display: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Drafting - original draft: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.
Writing - proofreading and editing: Lawrence Rodrigo Loaiza Solano, Luis Diego Moya Rojas, Sebastián Alejandro López Luna.

REFERENCES

1. Mallet P. Comparative analysis of data privacy legislation: convergence and divergence between the GDPR and CCPA. In: Studies in systems, decision and control. 2025. p. 465-475. https://doi.org/10.1007/978-3-031-84636-6_40

2. Wodi A. Artificial intelligence (AI) governance: an overview. SSRN Electron J. 2024. https://doi.org/10.2139/ssrn.4840769

3. Almeida D, Shmarko K, Lomas E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI Ethics. 2021;2(3):377-387. https://doi.org/10.1007/s43681-021-00077-w

4. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. Nat Mach Intell. 2019;1(9):389-399. https://doi.org/10.1038/s42256-019-0088-2

5. Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, et al. AI4People—An ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds Mach. 2018;28(4):689-707. https://doi.org/10.1007/s11023-018-9482-5

6. OECD. Governing with artificial intelligence. In: OECD Publishing eBooks. 2025. https://doi.org/10.1787/795de142-en

7. Jordanoski Z. The role of regulatory frameworks in shaping e-governance. Conf Digit Gov Res. 2025;1. https://doi.org/10.59490/dgo.2025.1037

8. Maslej N, Fattorini L, Brynjolfsson E, Etchemendy J, Ligett K, Lyons T, et al. Artificial intelligence index report 2023. arXiv. 2023. https://doi.org/10.48550/arxiv.2310.03715

9. Davtyan T. The U.S. approach to AI regulation: federal laws, policies, and strategies explained. SSRN Electron J. 2024. https://doi.org/10.2139/ssrn.4954290

10. Zhang AH. The promise and perils of China's regulation of artificial intelligence. SSRN Electron J. 2024. https://doi.org/10.2139/ssrn.4708676

11. Maslej N, Fattorini L, Perrault R, Parli V, Reuel A, Brynjolfsson E, et al. Artificial intelligence index report 2024. arXiv. 2024. https://doi.org/10.48550/arxiv.2405.19522

12. Maslej N, Fattorini L, Perrault R, Gil Y, Parli V, Kariuki N, et al. Artificial intelligence index report 2025. arXiv. 2025. https://doi.org/10.48550/arxiv.2504.07139

13. AllahRakha N. UNESCO's AI ethics principles: challenges and opportunities. Int J Law Policy. 2024;2(9):24-36. https://doi.org/10.59022/ijlp.225

14. Knöchel T, Schweizer KJ, Acar OA, Akil AM, Al-Hoorie AH, Buehler F, et al. Core principles of responsible generative AI usage in research. AI Ethics. 2025;5(6):6371-6377. https://doi.org/10.1007/s43681-025-00768-8

15. Göksal Şİ, Vasquez MCS, Chochia A. The EU AI Act's alignment within the European Union's regulatory framework on artificial intelligence. Int Comp Law Rev. 2024;24(2):25-53. https://doi.org/10.2478/iclr-2024-0017

16. Hine E, Floridi L. The blueprint for an AI Bill of Rights: in search of enaction, at risk of inaction. Minds Mach. 2023;33(2):285-292. https://doi.org/10.1007/s11023-023-09625-1

17. Tabassi E. Artificial intelligence risk management framework (AI RMF 1.0). 2023. https://doi.org/10.6028/nist.ai.100-1

18. Xu J. Opening the 'black box' of algorithms: regulation of algorithms in China. Commun Res Pract. 2024;10(3):288-296. https://doi.org/10.1080/22041451.2024.2346415

19. Shepherd T. The Canadian Clearview AI investigation as a call for digital policy literacy. Surveill Soc. 2024;22(2):179-191. https://doi.org/10.24908/ss.v22i2.16300

20. Kronqvist A, Rousi R. Gender-based cognitive bias and design thinking in the work of Finnish IT professionals. Inf Softw Technol. 2025;189:107910. https://doi.org/10.1016/j.infsof.2025.107910

21. Guadamuz A. The EU's artificial intelligence act and copyright. J World Intellect Prop. 2024;28(1):213-219. https://doi.org/10.1111/jwip.12330

22. Olimid AP. Legal analysis of EU artificial intelligence act (2024): insights from personal data governance and health policy. Access Justice East Eur. 2024;7(4):120-142. https://doi.org/10.33327/ajee-18-7.4-a000103

23. Monko GJ, Mjahidi MM. From bias to balance: navigating gender inclusion in AI. In: Artificial intelligence. 2024. https://doi.org/10.5772/intechopen.1007449

24. Jung WK, Kwon HY. Privacy and data protection regulations for AI using publicly available data: the Clearview AI case. ACM Digit Libr. 2024;48-55. https://doi.org/10.1145/3680127.3680200

25. Hanna M, Pantanowitz L, Jackson B, Palmer O, Visweswaran S, Pantanowitz J, et al. Ethical and bias considerations in artificial intelligence/machine learning. Mod Pathol. 2024;38(3):100686. https://doi.org/10.1016/j.modpat.2024.100686

26. National Institute of Standards and Technology. Artificial intelligence risk management framework. 2024. https://doi.org/10.6028/nist.ai.600-1

27. Wachter S, Mittelstadt B, Russell C. Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI. Comput Law Secur Rev. 2021;41:105567. https://doi.org/10.1016/j.clsr.2021.105567

28. Schwartz R, Vassilev A, Greene K, Perine L, Burt A, Hall P. Towards a standard for identifying and managing bias in artificial intelligence. 2022. https://doi.org/10.6028/nist.sp.1270

29. Gillespie N, Lockey S, Ward T, Macdade A, Hassed G. Trust, attitudes and use of artificial intelligence: a global study 2025. University of Melbourne Data Repository. 2025. https://doi.org/10.26188/28822919.v1

30. Bayan FMH. The ethics of AI: navigating the moral dilemmas of artificial intelligence. Arab J Sci Publ. 2024;7(66):1-11. https://doi.org/10.36571/ajsp661

31. Ghosh M. Artificial intelligence (AI) and ethical concerns: a review and research agenda. Cogent Bus Manag. 2025;12(1). https://doi.org/10.1080/23311975.2025.2551809

32. Shams RA, Zowghi D, Bano M. AI for all: identifying AI incidents related to diversity and inclusion. J Artif Intell Res. 2025;83. https://doi.org/10.1613/jair.1.17806

33. Hoofnagle CJ, Van Der Sloot B, Borgesius FZ. The European Union general data protection regulation: what it is and what it means. Inf Commun Technol Law. 2019;28(1):65-98. https://doi.org/10.1080/13600834.2019.1573501

34. Issaoui A, Örtensjö J, Islam MS. Exploring the general data protection regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. Future Bus J. 2023;9(1). https://doi.org/10.1186/s43093-023-00285-2

35. Ufert F. AI regulation through the lens of fundamental rights: how well does the GDPR address the challenges posed by AI? 2020. https://doi.org/10.15166/2499-8249/394

36. Kim B, Jeong S, Cho B, Chung J. AI governance in the context of the EU AI Act. IEEE Access. 2025;13:144126-144142. https://doi.org/10.1109/access.2025.3598023

37. Alimkhanov M. Comparative analysis of international AI regulatory approaches: the United States, European Union, Canada, China, Kazakhstan, Russia. SSRN Electron J. 2024. https://doi.org/10.2139/ssrn.4873053

38. Swaminathan N, Danks D. Application of the NIST AI risk management framework to surveillance technology. arXiv. 2024. https://doi.org/10.48550/arxiv.2403.15646

39. Dotan R, Blili-Hamelin B, Madhavan R, Matthews J, Scarpino J. Evolving AI risk management: a maturity model based on the NIST AI risk management framework. arXiv. 2024. https://doi.org/10.48550/arxiv.2401.15229

40. Goldman E. An introduction to California's consumer privacy laws (CCPA and CPRA). SSRN Electron J. 2021. https://doi.org/10.2139/ssrn.3896176

41. Roberts H, Cowls J, Hine E, Morley J, Wang V, Taddeo M, et al. Governing artificial intelligence in China and the European Union: comparing aims and promoting ethical outcomes. Inf Soc. 2022;39(2):79-97. https://doi.org/10.1080/01972243.2022.2124565

42. Vöneky S, Kellmeyer JP, Müller O, Burgard W. The Cambridge handbook of responsible artificial intelligence. In: Cambridge University Press eBooks. 2022. https://doi.org/10.1017/9781009207898

43. Zou M, Zhang L. Navigating China's regulatory approach to generative artificial intelligence and large language models. Cambridge Forum AI Law Gov. 2025;1. https://doi.org/10.1017/cfl.2024.4

44. Phillips PJ, Hahn CA, Fontana PC, Yates AN, Greene K, Broniatowski DA, et al. Four principles of explainable artificial intelligence. 2021. https://doi.org/10.6028/nist.ir.8312

45. Schwartz R, Fontana PC. The language of trustworthy AI. 2023. https://doi.org/10.6028/nist.ai.100-3

46. European Parliament. The white paper on artificial intelligence. 2020. https://doi.org/10.2861/614816

47. Ebers M, Hoch VRS, Rosenkranz F, Ruschemeier H, Steinrötter B. The European Commission's proposal for an artificial intelligence act—A critical assessment by members of the Robotics and AI Law Society (RAILS). J Multidiscip Sci J. 2021;4(4):589-603. https://doi.org/10.3390/j4040043

48. Gornet M, Maxwell W. The European approach to regulating AI through technical standards. Internet Policy Rev. 2024;13(3). https://doi.org/10.14763/2024.3.1784

49. European Data Protection Supervisor. AI Act regulation (EU) 2024/1689: regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Publications Office of the European Union; 2025. https://doi.org/10.2804/4225375

50. Roberts H, Cowls J, Morley J, Taddeo M, Wang V, Floridi L. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI Soc. 2020;36(1):59-77. https://doi.org/10.1007/s00146-020-00992-2

51. Migliorini S. China's interim measures on generative AI: origin, content and significance. Comput Law Secur Rev. 2024;53:105985. https://doi.org/10.1016/j.clsr.2024.105985

52. Choi C, Yoon J. AI policy in action: the Chinese experience in global perspective. J Policy Stud. 2025;40(2):1-23. https://doi.org/10.52372/jps.e685

53. Cao X, Power L. Controlled carefully: how consumer care legitimizes China's AI regulations. Inf Commun Soc. 2025:1-17. https://doi.org/10.1080/1369118x.2025.2474565

54. Al-Maamari A. Between innovation and oversight: a cross-regional study of AI risk management frameworks in the EU, U.S., UK, and China. arXiv. 2025. https://doi.org/10.48550/arxiv.2503.05773

55. Arora AS, Saboia L, Arora A, McIntyre JR. Human-centric versus state-driven. Int J Intell Inf Technol. 2025;21(1):1-13. https://doi.org/10.4018/ijiit.367471

56. Robinson L, Kizawa K, Ronchi E. Interoperability of privacy and data protection frameworks. OECD Going Digital Toolkit Notes. 2021. https://doi.org/10.1787/64923d53-en

57. Chun J, Schroeder DWC, Elkins K. Comparative global AI regulation: policy perspectives from the EU, China, and the US. arXiv. 2024. https://doi.org/10.48550/arxiv.2410.21279

58. Alic D. The role of data protection and cybersecurity regulations in artificial intelligence global governance: a comparative analysis of the European Union, the United States, and China regulatory framework. 2021 Oct 31. https://doi.org/10.13140/rg.2.2.29886.00328