JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 4083-4090
ISSN: 2589-1316

The Divergence of Legislative Models in Addressing Artificial Intelligence Crimes: A Comparative Study of the European Union, China, and the United States

Samer Saadoun Al-Amiri[1], Hajar Muqdad[2*]

[1] *University of Baghdad, College of Law,* IRAQ*; Email: Dr.samer@colaw.uobaghdad.edu.iq , https://orcid.org/0000-0002-7683-4445*

[2] *University of Baghdad, College of Law,* IRAQ*; Email: hajar.sayhood1600@colaw.uobaghdad.edu.iq , https://orcid.org/0009-0004-9996-3487*

***Corresponding Author:** hajar.sayhood1600@colaw.uobaghdad.edu.iq

Citation: Al-Amiri, S. S. and Muqdad, H. (2025). The Divergence of Legislative Models in Addressing Artificial Intelligence Crimes: A Comparative Study of the European Union, China, and the United States, *Journal of Cultural Analysis and Social Change*, 10(2), 4083-4090. https://doi.org/10.64753/jcasc.v10i2.2234

Published: November 22, 2025

ABSTRACT

The rapid advancement of artificial intelligence technologies has created unprecedented legal challenges in combating crimes arising from their unlawful use. This study analyzes comparative legislative frameworks for addressing ai-related crimes through three international models: the European union, which adopts a preventive risk-based approach; China, which implements a centralized strategy focused on digital sovereignty and national security; and the United States, which employs a decentralized system between federal and state levels. The study reveals fundamental divergences in legislative philosophies: the European model balances rights protection with innovation encouragement, the Chinese model links legitimacy to social stability, while the American model emphasizes direct criminal sanctions. The research emphasizes the necessity of international coordination to establish unified legal frameworks addressing the cross-border nature of these crimes and developing effective law enforcement mechanisms in modern cyberspace.

Keywords: Artificial Intelligence, Cybercrime, Criminal Legislation, Risk-Based Regulation, AI Governance, Rights Protection

INTRODUCTION

The rapid evolution of artificial intelligence (AI) has transformed it from a tool of innovation into a central force poses modern legal, economic, and security systems. Yet this technological progress has simultaneously generated new forms of crimes that traditional laws are often ill-equipped to address. Existing legal frameworks, designed for human-centered conduct, struggle to regulate autonomous, algorithmic, and transnational behaviours, revealing a widening gap between technological advancement and legal adaptation.

In response, numerous global and national initiatives have sought to establish frameworks for AI governance. However, most of these remain in their preliminary stages, grounded primarily in ethical guidelines and soft-law principles rather than enforceable legal norms. While such efforts provide valuable moral orientation, they lack the institutional mechanisms and accountability structures necessary for effective regulation. Hence, examining the most advanced legislative experiences becomes essential to understand how legal systems can evolve from ethical aspirations to binding norms.

This study focuses on three of the most developed and influential legal models addressing ai-related crimes: the european union, the people's republic of china, and the united states. These models have advanced further

than others in transforming theoretical principles into applicable legal mechanisms and therefore serve as useful references for comparative analysis in the search for more coherent global regulation.

The research employs a comparative analytical methodology, through the examination of legislative texts, official documents, and regulatory instruments within the three selected models, comparing their respective approaches to identify common foundations, divergences, and best practices. By analysing the strengths and limitations of these frameworks, the study aims to contribute to the development of a coherent international legal vision capable of ensuring both innovation and accountability in the age of artificial intelligence.

The European Union Model

The European union considered one of the most important regions that took advanced organizational steps to confront legal, moral and economical challenges arising from using artificial intelligence technology ,on the contrary from the international frameworks that restricted mostly to not binding recommendation to the countries, the European union came with comprehensive and binding law called "ai act" that approver by the European parliament in 13 march 2024 ,to form the first comprehensive and legal framework of its kind on global level.(European Union, 2024; Ağdemir et al., 2025; Agnihotri, 2022; Adawiah, 2022; Belhaj, 2025)

The Risk-Based Classification Of AI Systems

This act reflects strategic European vision based on the principle of *"risk-based approach"*, so legal obligation is imposed proportionate with the potential risk level for each kind of systems (Sousa E Silva, 2024: P.28; Derakhshani et al., 2025; Udemezue et al., 2025), so the systems classified in this act to four main categories:

Unacceptable Risk Systems: systems whose use is strictly prohibited and which may not be deployed or operated within the European union under any circumstances, such as crime prediction systems and biometric recognition systems in public places without judicial permission. (European Union, 2024: Art. 5; Abdul et al., 2025)

High Risk Systems: that allowed to use in the European market under strict regulatory terms and obligations, including applications in sensitive sectors such as criminal justice and ai-enhanced vehicles. (European Union, 2024: Arts. 6-15)

Limited Risk Systems: this category include the systems that doesn't pose a significant risk on basic rights, but pose transparency requirements, such as deep fake [1] and recommendations systems. (Al-Najar, 2024: P. 559; Moschogianni, 2025; Shamsuddin, 2025)

Low Risk Systems: that doesn't pose any significant danger to individuals' rights or safety, such as games based on ai or unwanted e-mail filters, so dose not submit to any specific system. (European Union, 2024: Art. 95; Istiarto et al., 2023; Huhemandula et al., 2025; Batool et al., 2024)

Executive Guarantees and Accountability in the (AI Act)

This category involve many important advantages, its balance between human rights protection and encouraging innovation, it also pose clear obligations on the developers and the users regarding transparency and documentation as well as conformity assessment and registration mechanisms which allow the supervisory authorities to watch systems performance, Besides that, the act adapt preventive and accounting accountability-based system, that distribute responsibilities among various parties involved to guarantee no party should be escapes legal liability, and specifies severe financial penalties up to 35 million euro or 7% of total annual revenue for those who violate the law (European Union, 2024: Art. 99), these obligations and penalties reflect the seriousness and strictness with which the european union regulates AI, even though it has not yet reached the stage of imposing criminal sanctions.

This act goes with wider frame include accompanying legislation like general data protection regulation (GDPR),that enhance the personal data used to train AI algorithms ,so its imposes preventive principles like `safety by design' which mean collect the data for explicit and legitimate specific purposes and 'data minimizing' that require the analyzed data to be suitable and of limited relevance to what is necessary for the intended purposes(European Union, 2016' An, 2022), which considered necessary to confront the illegal use of AI.

So the measures and the act together forms cohesive system that insure reducing violation, and enhance individuals rights in complex digital environment . And hence it becomes clear to us that the european experience provide applicable and inspiring model for other regions, for what it contain of strict legal balance and innovation encouragement, which explain the european national legislative authorities attention to adapt its local laws with

[1] This refers to an artificial intelligence-based technology used to generate images, videos, or audio recordings that closely resemble real ones. The technology relies on deep learning algorithms, particularly Generative Adversarial Networks (GANs), which reconstruct features or sounds to produce a version difficult to distinguish from reality, making it a controversial tool due to its potential use in misinformation or digital crimes.

this model, as shown in recent legislative initiatives in countries such as Italy, which enacted law no. 132/2025 in September 2025, becoming the first EU state to implement the AI act nationally. The law criminalizes deepfake content distribution (1-5 years' imprisonment), considers ai use an aggravating circumstance in traditional crimes (up to 7 years), and imposes substantial fines reaching six million euros (Italian Republic, 2025) and Spain[2] (Linklaters LLP, 2025) France[3]. (Bird & Bird LLP, 2025; Ismail, 2025)

The People's Republic of China Model

China considered one of the leading countries globally in the development and use of AI technology, so its invested intensely in research and development and occupied an advanced position in this biotechnical field, and as a response to this leadership China adapt strict central legal frame aims to organize the use of this technologies and protect the national security and social system, and follows gradual strategy based on two main axes which are: fundamental laws, and regulatory measures.

Fundamental Laws

The legal regulation of AI in China derived its strength from three central laws which is: cyber security law and data security law and personal information protection law, that reflect the 'digital sovereignty' concept as foundation in legislative policy to confront the risks related to AI technology.

The cyber security law in 2017 imposes strict restrictions on transport sensitive data related to critical infrastructure or biometric information to prevent using it in training AI systems (National People's Congress, 2017: Art. 37), with obligating network operators to adopt technical oversight systems to monitor the threats and immediate reporting on any violation (Creemers, 2021: P.119; Kahil, 2025; Katsamba, 2025), and hence guarantee to track the data path and stop the widespread abuse by AI systems.

As for data security law (2021) it came complementing to its previous and stand out from it by expanding the frame of legal protection by classify the data according to risk level and impose gradual security measures accordingly(National People's Congress, 2021a: Art. 21) it also classify how to deal with the data based on its sensitivity (Filipova, 2024: P.51) and impose financial sanctions that may reach to millions yuan in case of serious damage occurs and punish the mediators who trade the illegal data with fines that reach tenfold the illegal profit. (National People's Congress, 2021a: Arts. 45, 47, 4; Benjar et al., 2023) .

While personal information protection law (2021) follows similar approach to what was reported in the European general data protection regulation (GDPR) by obligating the developers to set clear legal purpose for data collecting, and get explicit consent from the individuals before collecting their personal information and use it including the data that processed within the AI systems. (National People's Congress, 2021b: Arts. 6, 13)

And by that these three laws forms integrated legal system aims to adjust the flow of data and protect it from unlawful exploitation, and put clear boundaries to use the personal data in developing and operating AI systems, but it remains limited in data frame only without extending to other AI systems axes.

Regulatory Measures

As for measurements level China has made advanced step by issue list of (Deep generating management of AI) in 2023 to confront digital crimes associated with (Deepfake), and include the applications that use algorithms to adjust or construct texts, photos, videos and audios (Cyberspace Administration of China, 2022: Art. 17), and the measurements impose obligations on content generation services platforms providers the necessity of disclosure on their data algorithms and ensure transparency and tag the content produced by AI and require the final users not to use these technologies to produce prohibited or misleading information(Cyberspace Administration of China, 2022: Arts. 6, 9)

China also issued the first legal frame to organize generative AI services in a comprehensive manner in 2023 which is (Interim Measures For The Management Of Generative Artificial Intelligence Services), so it was more comprehensive and strict from its predecessors by obligating the service providers to bear the direct responsibility on the security of produced content and fulfil the obligations related to personal data protection and clearly define the generated content, as well as create effective mechanisms to report complaints and monitor violations and report it to the cometent authorities. (Cyberspace Administration of China, 2023: Arts. 4, 11, 13; Ghasemi et al., 2025)

[2]The Spanish government approved a draft bill imposing heavy fines of up to €35 million or 7% of annual revenue on companies using AI-generated content without clear labeling, classifying such acts as serious violations, including deepfakes that threaten democracy and institutional trust.

[3] France Has Developed Sector-Specific Legislation requiring AI-generated image labeling on social media, with fines up to €3,750 for individuals and €50,000 for platforms.. See: European AI Regulatory Horizon Tracker: France. Bird & Bird LLP, updated 30 June 2025 . Available

In 2024 it adopt regulation proposal specialized in AI known as (expert proposal), aims to regulate AI and accountability for the misuse of its systems(Massatuly, 2024: P.305), similar to European union act for AI this proposal identifies critical systems such as those used in informatics infrastructure and systems affecting personal rights and foundation models with high abilities and impose strict obligations on it to guarantee safety and security (Center for Security and Emerging Technology, 2024: Arts. 7, 17, 23-25), and expand the proposal from the scope of application to include the activities outside the Chinese borders in case it affects the citizens or national security of the country (Saiapin, 2025: P.25), and the financial fines reaches millions yuan on the violators as well as suspension or cancellation of the permissions and licenses and fines the responsible individuals on the violations, the proposal also admits the importance of corporate compliance system in mitigation of criminal liability. (Center for Security and Emerging Technology, 2024: Arts. 68, 69; Abdullahi, 2025)

And by that the regulatory measures completed what the fundamental laws began, to transmit from data protection to regulate AI systems itself and identify the responsibilities of the providers and the users.

The United States Model

The United States adopts a decentralized approach to addressing the risks of AI system misuse, with the regulatory response distributed across federal statutes, state laws, and executive orders. And despite the absence of comprehensive unified law, the federal government has taken extensive regulatory measures to ensure the safe use of this technology at both federal and state levels.

Federal Level Legislation

Executive Orders

The U.S. executive orders on AI regulation reveal a contradictory strategy, reflecting a fundamental conflict between safety and innovation. This began under the Biden administration, which adopted a 'safety-first' approach through Executive Order No. 14110 (2023), warning of the risks of accelerated development without sufficient safeguards.(Executive Order 14110, 2023)However, this approach shifted with the return of the Trump administration, which considered this approach as an obstacle to U.S. technological supremacy and revoked his predecessor's policies, issuing Executive Order No. 14179 and declaring a 'barrier-free' as new philosophy for global leadership.(Executive Order 14179, 2025; Yen et al., 2020)

These political fluctuations reveal a deep strategic dilemma: how can a country maintain technological leadership without compromising safety, especially when competing powers such as China demonstrate a more consistent and long-term planning approach.

Federal Legislation

U.S. federal legislation in addressing AI- related crimes represents a gradual evolutionary process of reliance on typical, non-specialized laws to building a specific legal framework to confront contemporary challenges.

In recent years, there has been a qualitative development in specialized legislation. The United States was the first country to respond legislatively to deepfake technology through the (DEEPFAKES Accountability Act) which has been reintroduced in an updated form in September 2023. This law is comprehensive, covering all types of deepfakes by requiring the addition of visible watermarks and labels on all AI-generated content, with penalties of up to five years' imprisonment and compensations of $150,000 per violation. (Congress.gov, H.R.5586 - 118th Congress, 2023) . However, it faces resistance from tech companies due to implementation costs and the technical complexity of addressing all forms of deepfakes.

In contrast, in 2025, Congress passed the TAKE IT DOWN Act, to become the first federal law explicitly criminalizing the distribution of realistic intimate images of real individuals without their consent, whether actual or AI-generated. The law imposes penalties of up to three years' imprisonment and fines, and obliges digital platforms to remove the offending content within 48 hours of notification by the victim. (Congress.gov, S.146 - 119th Congress, 2025), Despite its effectiveness, the law is limited to pornographic deepfakes and does not cover other forms of deepfakes, making its scope narrower compared to the DEEPFAKES Accountability Act, which addresses these gaps through its broader applicability.

Legislative efforts have also expanded to include the institutional and technical framework for AI use through the Federal AI Risk Management Act (2023), which aims to regulate AI deployment within federal agencies by developing an integrated risk assessment mechanism for sensitive sectors. (Congress.gov, S.3205 - 118th Congress, 2023), Additionally, the Algorithmic Accountability Act (2022) focuses on automated decision-making systems. Under Section 3, companies are required to conduct comprehensive risk assessments and ensure full transparency in algorithmic operations, thereby establishing a preventive framework against algorithmic discrimination and manipulation (Mökander et al., 2022: PP.752-753; Falaqi, et al., 2025)

Currently, the AI Whistleblower Protection Act is being proposed, aiming to empower employees to report AI system misuse without fear of workplace retaliation. (Congress.gov, S.1792 - 119th Congress, 2025; Ndububa

et al., 2025). These legislative developments reflect a gradual shift from a limited response focused on specific issues, such as pornographic deepfakes, toward a more comprehensive approach through bills designed to provide broader coverage and impose advanced oversight mechanisms. Nevertheless, these efforts still face challenges related to the rapid pace and complexity of AI development, raising the fundamental question: can this fragmented legal framework keep pace with accelerating technological progress, or is there an urgent need for a single, unified legislation to consolidate these scattered efforts?

State Legislation

At the state level, numerous initiatives have emerged in the absence of a unified federal law, reflecting the decentralized U.S. system in addressing AI challenges. California leads these efforts through the (California Consumer Privacy Act), which requires developers to disclose data collection and usage practices and imposes fines of up to $7,500 per intentional violation(California Civil Code, 2018). New York has adopted a stricter approach with the (New York Privacy Act), focusing on corporate duties in risk assessment and granting individuals the right to access, correct, and delete their data used in AI systems. (New York State Senate, 2023)

Colorado preceded many states with the Colorado Artificial Intelligence Act (2024), which employs a risk-based approach similar to the European model, imposing transparency standards, requiring reporting of algorithmic bias within 90 days, and obliging distributors to inform users when interacting with AI systems .(Colorado General Assembly, 2024)

Deepfake-related offenses have been a central issue in state legislation since 2019. Virginia was the first to amend its law to include deepfakes as a first-degree misdemeanor, with penalties of up to one year imprisonment and fines of $2,500 (Virginia General Assembly, 2019; Hussain et al., 2024; Abbas et al., 2024). California followed with two notable laws: AB 602 (AB-602, 2019-2020), criminalizing non-consensual sexual deepfake images, and AB 730 (AB-730 2019-2020), protecting candidates from manipulated content within 60 days before elections. However, their limited scope, targeting specific groups only, has raised concerns regarding legal coverage fairness (Abu Alaa, 2024: P.501; Hussain et al., 2025; Noor, 2022; Salleh et al., 2023; Haokip, 2025). Texas enacted a similar electoral law criminalizing the distribution of manipulated videos against candidates within 30 days of elections, with penalties of up to one year imprisonment and fines of $4,000 (Al-Najar, 2024: P.596) .

Subsequently, other states including Missouri and New York (2020), Minnesota and Mississippi for political deepfakes, and Utah, Rhode Island, and North Carolina (2023) joined these efforts. Nevertheless, these state-level initiatives exhibit significant variation in focus between sexual and political deepfakes. (Ballotpedia, 2025: 5-14)

CONCLUSION

This Study Has Examined The Divergence Of Legislative Models In Addressing Artificial Intelligence Crimes Through A Comparative Analysis Of The European Union, China, And The United States. By Applying A Comparative Analytical Methodology To Legislative Texts And Regulatory Documents, The Research Demonstrates That Each Model Reflects Distinct Socio-Political Priorities In Regulating AI Systems.

The European Union Has Adopted A Comprehensive Risk-Based Approach Through The AI Act, Which Provides Legal Clarity In Defining Prohibited Acts And Penalties While Carefully Balancing Rights Protection With Innovation encouragement Through Administrative Sanctions And Technical Risk Classification. This Approach Represents Legislative Maturity, Though It Remains Hindered By Bureaucratic Complexity. In Contrast, China Has Implemented A Centralized Gradual Strategy That Began With General Security Laws, Progressively Evolved Into Specialized Regulations Targeting Deepfakes And Generative AI, And Currently Pursues Unified Legislation Through A Draft Law That Remains Unenacted. This Model Prioritizes Digital Sovereignty And Social Stability Through Strict Preventive Oversight With Flexible Risk Definitions Linked To Public Opinion Impact.

Meanwhile, The United States Employs A Fragmented Decentralized System That Distributes Authority Between Federal And State Levels, Demonstrating Clear Superiority In Direct Criminal Sanctions Including Imprisonment And Substantial Fines For Specific Offenses Such As Deepfakes. However, This Strength Is Constrained By Legislative Fragmentation And Excessive Economic Caution Toward Corporate Interests.

These Findings Reaffirm That Effective AI Governance Requires Integrating Preventive, Punitive, And Sovereign Dimensions, As Legislative Effectiveness Depends Not Only On Textual Rigor But Also On Technical Enforcement Capacity, International Cooperation Mechanisms, And Adaptive Responsiveness To Technological Evolution. This Research Thus Contributes To Scholarship On Transnational Digital Governance While Offering Practical Lessons For Nations Developing Their Own Regulatory Frameworks. Future Research Should Examine How These Models Evolve As AI Advances Toward Greater Autonomy And Whether International Harmonization Efforts Produce Convergence Or Further Divergence. Ultimately, The Study Underscores That Addressing AI Crimes Effectively Requires Recognizing AI's Autonomous Decision-Making Potential, Thereby

Necessitating Innovative Legal Constructs That Can Accommodate Both Corporate Liability And Emerging Concepts Of Electronic Legal Personality In Global Cyberspace.

REFERENCES

Abbas, A., Hussain, T., Hussain, H., Arif, S., & Batool, S. (2024). Navigating urban environmental hazards: policies and pathways to health equity in Pakistan within the framework of sustainable development goals. Journal of Management Practices, Humanities and Social Sciences (JMPHSS)., 8(6), 16-24.

Abdul Jabbar Al-Sammak, M., Ahmed Al-Hamamy, M., & Khuder Yaqoob, M. (2025). The role of open knowledge management in driving marketing innovation within organizations: The mediating role of technology empowerment. Problems and Perspectives in Management, 23(4), 75–89. https://doi.org/10.21511/ppm.23(4).2025.06

Abdullahi, B. (2025). Impact of N-power program on poverty alleviation in Nigeria: A study of Gombe State. Journal of Advances in Humanities and Social Sciences, 11(2). https://doi.org/10.20474/jahss-11.2.1

Abu Alaa, Ashraf S. (2024). Criminal Confrontation of Deepfake Technology. Journal of Legal and Economic Sciences, 66(3), 477–511. Https://doi.org/10.35246/9sjgyd13

Adawiah, R. (2022). Factors that influence the compliance of medical record filling by nurses in inpatient of Regional General hospital Dr. H. Moch. Ansari Saleh Banjarmasin. Journal of Advances in Health and Medical Sciences, 8(1). https://doi.org/10.20474/jahms8.2

Ağdemir, E., Kuyucu, M., Yücedağ, M., & Ağdemir, K. K. (2025). Assessment of Xenopsin Related Peptide-1 levels in pregnant women with gestational diabetes mellitus. Perinatal Journal, 33(1), 5-10.

Agnihotri, V. (2022). Paradigm Shifts from Social Forestry to Urban Forestry: A Synergy to Mitigate Urban Heat Island in High-Density Developments. Journal of Applied and Physical Sciences, 8. https://doi.org/10.20474/japs-8.4

Al-Najar, Sahar Fouad Majeed. (2024). Criminal Response to Crimes Stemming from the Use of Deepfake Technology. Journal of Legal Science, 39(2), 501–596. Https://doi.org/10.35246/9sjgyd13

An, X. (2022). Computerization in the study of Athenians. Journal of Applied and Physical Sciences, 8(1). https://doi.org/10.20474/japs-8.3

Ballotpedia. (2025). State of Deepfake Legislation: 2025 Mid-Year Report. Washington, D.C.: Ballotpedia. Available at: https://ballotpedia.org/Ballotpedia%27s_State_of_Deepfake_Legislation_2025_Annual_Report (Accessed 20 October 2025).

Batool, A., Batool, I., & Aziz, A. (2024). The effect of emotional intelligence and leadership skills on organizational commitment: A case study of civil servants. Journal of Management Practices, Humanities and Social Sciences, 8(3), 164-173.

Belhaj, S. (2025). The Influence of Student-Generative AI Interaction on Self-Regulated Learning and Academic Achievement. Journal of Advanced Research in Social Sciences and Humanities, 10(4), 28-41.

Benjar, Z. G., & Zarandi, M. M. (2023). Evaluated Of playground quality according to comforta-bility for healthy and disabled children case study: Mel-lat park, Qazvin, Iran.

Bird & Bird LLP. (2025, June 30). European AI Regulatory Horizon Tracker: France. London: Bird & Bird LLP. Available at: https://www.twobirds.com/en/capabilities/artificial-intelligence/ai-legal-services/ai-regulatory-horizon-tracker/france (Accessed 3 October 2025).

California Civil Code §§ 1798.100–1798.105. (2018). California Consumer Privacy Act (CCPA). Sacramento, CA: California State Legislature. Available at: https://cdp.cooley.com/ccpa-2018/ (Accessed 20 October 2025).

California Legislative Information. (2019-2020). AB-602: Depiction of an Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action. Sacramento, CA: California Legislative Information. Available at: https://leginfo.legislature.ca.gov/faces/billstatusclient.xhtml?Bill_id=201920200AB602 (Accessed 19 October 2025).

California Legislative Information. (2019-2020). AB-730: Elections: Deceptive Audio or Visual Media. Sacramento, CA: California Legislative Information. Available at: https://leginfo.legislature.ca.gov/faces/billstatusclient.xhtml?Bill_id=201920200AB730 (Accessed 19 October 2025).

Center for Security and Emerging Technology (CSET). (2024, March). Translation: Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars). Washington, D.C.: Georgetown University. Available at: https://cset.georgetown.edu/publication/china-ai-law-draft/ (Accessed 10 October 2025).

Colorado General Assembly. (2024). Colorado Artificial Intelligence Act, SB 24–205 (2024), §§ 6-1-1701 to 1707. Denver, CO: State of Colorado. Https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_205_enr.pdf

Congress.gov. (2020). National Artificial Intelligence Initiative Act, H.R. 6216, 116th Congress. Washington, D.C.: U.S. Government Publishing Office. Available at: https://www.congress.gov/bill/116th-congress/house-bill/6216 (Accessed 7 October 2025).

Congress.gov. (2023). H.R. 5586 - 118th Congress: DEEPFAKES Accountability Act. Washington, D.C.: U.S. Government Publishing Office. Available at: https://www.congress.gov/bill/118th-congress/house-bill/5586/text. (Accessed 13 October 2025).

Congress.gov. (2023). S.3205 - 118th Congress: Federal Artificial Intelligence Risk Management Act of 2023. Washington, D.C.: U.S. Government Publishing Office. Available at: https://www.congress.gov/bill/118th-congress/senate-bill/3205/ (Accessed 10 October 2025).

Congress.gov. (2025). S.146 - 119th Congress: TAKE IT DOWN Act. Washington, D.C.: U.S. Government Publishing Office. Available at: https://www.congress.gov/bill/119th-congress/senate-bill/146 (Accessed 9 October 2025).

Congress.gov. (2025, May 15). S.1792 – 119th Congress: AI Whistleblower Protection Act. Washington, D.C.: U.S. Government Publishing Office. Available at: https://www.congress.gov/bill/119th-congress/senate-bill/1792/text (Accessed 19 October 2025).

Creemers, R. (2021). Cybersecurity law and regulation in China: Securing the smart state. China Law and Society Review, 6, 119–135. Https://doi.org/10.1163/25427466-06020001

Cyberspace Administration of China. (2022). Provisions on the Administration of Deep Synthesis of Internet Information Services. Beijing: CAC. Retrieved from https://perma.cc/JE3W-PF26 (Accessed 10 October 2025).

Cyberspace Administration of China. (2023). Interim Measures for the Management of Generative Artificial Intelligence Services. Beijing: CAC. Https://cyrilla.org/api/files/1728288405530qs2ud3o27ys.pdf

Derakhshani, A., Ghadi, A., & Vahdat, S. E. (2025). Effect of Chemical Additives on Carbon Dioxide in the Sustainable Production of Portland Pozzolanic Cement. Environment and Water Engineering, 11(1), 11-18.

European Union. (2016, May 4). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal of the European Union, L 119. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (Accessed 20 October 2025).

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act). Official Journal of the European Union, L 234. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (Accessed 20 October 2025).

Executive Order 14110. (2023, October 30). Safe, secure, and trustworthy development and use of artificial intelligence. Federal Register. Washington, D.C.: The White House. Available at: https://www.federalregister.gov/d/2023-24283 (Accessed 4 October 2025).

Executive Order 14179. (2025, January 23). Removing barriers to American leadership in artificial intelligence. Federal Register. Washington, D.C.: The White House. Available at: https://www.federalregister.gov/d/2025-02172 (Accessed 4 October 2025).

Falaqi, M. R., Tricahyo, A., & Ainiy, N. (2025). The development of Arabic calligraphy in Indonesia. Journal of Advances in Humanities and Social Sciences, 11(1). https://doi.org/10.20474/jahss-11.1.2

Filipova, I. A. (2024). Legal regulation of artificial intelligence: Experience of China. Journal of Digital Technologies and Law, 2(1), 51–68. Https://doi.org/10.21202/jdtl.2024.4

Ghasemi, F., & Zakaei, M. S. (2025). The challenges of the family in the digital age on a global level. Journal of Advances in Humanities and Social Sciences, 11(2). https://doi.org/10.20474/jahss-11.2.2

Haokip, S. (2025). Manipur Conflict: An analysis of causes, Claims by Meiteis and the State Government, and Counterclaims by Kukis. Journal of Advances in Humanities and Social Sciences, 11(1). https://doi.org/10.20474/jahss-11.1.3

Huhemandula, J. L., Bai, J., & Zaman, U. (2025). Responsibility Climate and Graduate Creativity in Higher Education: The Mediating Role of Learning Climate and the Moderating Effects of Teaching Strategies.9(4)-204 217.

Hussain, A., Sher, A., Khan, I. H., & Kanval, N. (2025). Evaluating Awareness and Knowledge about Tuberculosis: A Pathway to Improved Disease Management. Journal of Political Stability Archive, 3(2), 471-479.

Hussain, S., Hussain, I., Nasir, M. I., & Munaf, S. (2024). Bridging education and industry for enhanced corporate competency and economic development. Journal of Management Practices, Humanities and Social Sciences, 8(4), 40-50.

Ismail, S. (2025). Competencies and Stakeholder Engagement: Moderating the Relationship between Enterprise Social Media and Organizational Outcomes. Journal of Administrative and Business Studies, 11(1). https://doi.org/10.20474/jabs-11.1.3

Istiarto, I., Husaini, H., Marlinae, L., Suhartono, E., Suhartono, E., & Noor, M. S. (2023). Meta-analysis study: Relationship of age and workload of nurses in hospital. Journal of Advances in Health and Medical Sciences, 9(1). https://doi.org/10.20474/jahms-9.5

Italian Republic. (2025, September 25). Law No. 132/2025: Provisions and Delegations to the Government in the Field of Artificial Intelligence. Official Gazette of the Italian Republic, General Series, No. 223. Available at: https://www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/SG (Accessed 8 October 2025).

Kahil, B. (2025). Pathways to success: Exploring the mediating roles of affective learning and intellectual engagement in academic achievement. Journal of Advanced Research in Social Sciences and Humanities, 10(2), 27-38.

Katsamba, D. (2025). The Digital Nexus of Creativity: Mediating Roles of Self-Competence and Self-Efficacy in AI Use and Digital Literacy. Journal of Advanced Research in Social Sciences and Humanities, 10(3), 80-93.

Linklaters LLP. (2025). Spain Proposes a New AI Bill Including Significant Fines. Techinsights by Linklaters. Available at: https://techinsights.linklaters.com/post/102k3rk/spain-proposes-a-new-ai-bill-including-significant-fines (Accessed 5 October 2025).

Massatuly, A. (2024). China's Draft Expert AI Law: Towards accountability and safety in AI systems. Asian Law Review, 11(1), 72–90.

Mökander, J., Juneja, P., Watson, D., Floridi, L. (2022). The US Algorithmic Accountability Act of 2022 vs The EU Artificial Intelligence Act: What Can They Learn from Each Other? Minds & Machines, 32, 751–777. Https://doi.org/10.48550/arxiv.2407.06234

Moschogianni, G. (2025). Pathways to team performance and reduction of silence behaviour: Exploring the role of benevolent leadership through moderating impact of corporate social responsibility. Journal of Management Practices, Humanities and Social Sciences, 9(2), 93-106.

National People's Congress. (2017). Cybersecurity Law of the People's Republic of China. Beijing: NPC. Https://www.chinastandards.net/pdf_preview/cybersecuritylaw2017.pdf

National People's Congress. (2021). Personal Information Protection Law of the People's Republic of China. Beijing: NPC. Https://www.china-briefing.com/news/wp-content/uploads/2021/08/Personal-Information-Protection-Law-of-the-Peoples-Republic-of-China.pdf

Ndububa, C. L., & Ugoala, B. (2025). An analysis of contextual adaptation in ChatGPT's language use. Journal of Advances in Humanities and Social Sciences, 11(1). https://doi.org/10.20474/jahss-11.1.1

New York State Senate. (2023). New York Privacy Act, S.6701, §§ 1102–1107. Albany, NY: State of New York. Available at: https://www.nysenate.gov/legislation/bills/2021/S6701 (Accessed 11 October 2025).

Noor, E. S. (2022). The effect of convalescent plasma administration on increasing blood IGG and IGM levels as an effort to prevent death due to Covid-19 in ICU Panglima Sebaya hospital, Paser Regency, East Kalimantan. Journal of Advances in Health and Medical Sciences, 8(1). https://doi.org/10.20474/jahms-8.1

Saiapin, A. (2025). Cross-border regulation of artificial intelligence under China's Draft Expert Law. International Journal of Cyber Law, 19(3), 211–230.

Salleh, N. A., Shah, A., Mat, C. R. C., Talpuro, S. R., Ali, N. I., & Ali, H. B. Y. (2023). An integrated model of advanced artificial intelligence capability in higher education. Journal of Advances in Technology and Engineering Research, 8(2). https://doi.org/10.20474/jater-8.2.1

Shamsuddin, N., & Raza, S. (2025). Analyzing Peace Narratives: Content Analysis of Pakistan Studies Curricula and Textbooks at Secondary and Higher Secondary Levels. Journal of Management Practices, Humanities and Social Sciences, 9(1), 45-57.

Sousa E Silva, N. (2024). The Artificial Intelligence Act: Critical Overview. JIPITEC, 16(1), pp.1-36.

Udemezue, N., Unachukwu, U., & Nneli, C. (2025). Interconnectedness between stock market and economic growth in Nigeria: Evidence from Yamamoto and pairwise approaches. Journal of Administrative and Business Studies, 11(1). https://doi.org/10.20474/jabs-11.1.1

Virginia General Assembly. (2019). Virginia Code § 18.2–386.2 (Amended 2019). Richmond, VA: Commonwealth of Virginia. Available at: https://legiscan.com/VA/text/SB1736/id/1972006 (Accessed 19 October 2025).

Yen, C.-H., Lin, C.-H., Lin, J.-M., & Su, C. (2022). Design and application of unloaded flat transformers with spiral coils. Journal of Advances in Technology and Engineering Research, 8(1). https://doi.org/10.20474/jater-8.1.1

