Deepfakes and the Limits of Law: A Comparative Analysis of Regulatory Frameworks in the U.S., EU, and China

Christine Lumen
Independent Researcher, New York University
New York, NY, USA

ABSTRACT

The prolific rise of deepfakes has introduced new concerns, which in turn has intensified calls for a universal framework and more robust regulatory measures. Yet global regulatory responses remain fragmented. This paper investigates why regulatory divergence persists by integrating comparative legal analysis with Hofstede's Cultural Dimensions Theory. This paper is based on legislative frameworks from the United States, the European Union, and China and analyzes enforcement practices and cultural factors that shape regulatory design. The findings show that cultural values, such as power distance, individualism–collectivism, and uncertainty avoidance, significantly shape each region's tolerance for intervention and enforcement styles. The paper argues that harmonization cannot rely on uniform laws.

Methodologically, the paper adopts a comparative legal analysis combined with Hofstede's cultural dimensions theory to explain how national values shape what regulatory solutions are considered politically and socially legitimate.

The paper contributes to ongoing debates by demonstrating the need for cross-border hybrid regulatory models that balance innovation, human rights, and accountability.

Keywords

Deepfakes, synthetic media, deepfake regulation, AI governance, hybrid regulatory frameworks, cross-cultural regulation, Hofstede's cultural dimensions, comparative legal analysis.

1. INTRODUCTION

The roots of deepfakes technology are based on Generative Adversarial Networks, with the overall idea of generating synthetic information through machine learning that will resemble the real one [1]. This technology was introduced in 2014, while the term "deepfake" was first used in 2017, on Reddit where pornographic videos were shared with fake realistic-looking celebrities' faces on them [2]. Since then, the use of deep fake expanded beyond pornography to manipulation with information and, as a result, contributed to a growing decline in public trust in news media [7]. Headlines such as "You thought fake news was bad? Deep fakes are where truth goes to die" from Guardian or "'Deepfakes' are here. These deceptive videos erode trust in all news media" from The Washington Post show how deepfakes have elevated the threat of falsified media to an unprecedented scale and scope [4], [5]. Moreover, this trend was accompanied by tech gurus and executes about the threat posed by deepfakes in their open letter. In particular, Brad Smith, the vice president of Microsoft, wrote that: "We need to think early on and in a clear-eyed way about the problems that could lie ahead. As technology moves forward, [we need] to ensure proper control over AI [and] governments … need to move faster" [6]. This statement may be understood either as a genius call for tighter regulations or as a part of fear-driven narratives about new technologies. Yet, regulators remain reluctant to respond and adequately address legal gaps. Traditional statues on defamation, impersonation, or digital fraud were not designed to handle the speed with which deepfakes can spread.

This paper argues that the fragmented regulatory approaches to deepfakes—shaped by divergent cultural and legal traditions—undermine the possibility of effective unified legal framework. The analysis concludes that the only way forward is the adoption of a model that balances freedom of expression with accountability mechanisms, which can effectively address the risks posed by deepfake technologies.

2. METHODOLOGY

The research is based on a comparative and interdisciplinary methodology. First, it conducts a legal analysis of regulatory approaches to deepfakes in the United States, European Union, and China, with an emphasis on legislative drafts and policy reports. This comparative framework highlights differences in liability and enforcement that contribute to fragmented governance. Second, the paper applies Hofstede's Cultural Dimensions Theory to examine how national values, such as power distance, individualism-collectivism and uncertainty avoidance, influence regulatory choices and enforcement styles.

To support cross-national comparison, the study also develops a regulatory scoring framework used in Figures 2 and 3 Each jurisdiction was evaluated across enforcement power, transparency requirements and platform liability through a qualitative 1–5 scale. Scores were assigned according to statutory language, governance mechanisms, and observed enforcement practices (see Figure 1). Each domain was coded according to relative strength, where "1" represents minimal or no regulation and "5" corresponds to strong and comprehensive enforcement mechanisms. Intermediate values (2, 4) reflected partial coverage or limited institutional capacity. For the scenario-based assessment, law coverage (0 – 2) and enforcement severity (0–3) were coded for each harm category and combined into a 0 – 5 scenario score. With the coding scheme: 0 = no real enforcement, 1 – 2 = civil and administrative liability and 3 = criminal liability with significant penalties. Power Distance Index (PDI) and Uncertainty Avoidance Index (UAI) were taken from Geert Hofstede's Cultural Dimensions Theory. As for the European Union, index values were calculated as the average across member states to ensure consistency in further comparison.

Finally, the combined legal and cultural findings create a set of normative recommendations for a hybrid governance model that balances freedom of expression with accountability mechanisms.

3. LITERATURE REVIEW

Existing scholarship has approached the problem of deepfakes from several angles. Citron and Chesney warn that deepfakes threaten democratic processes through what they term the "liar's dividend" [7]. As it contributes to the spread of disinformation and undermining public trust in institutions. By contrast, Lindsey Wilkerson emphasizes the danger of overregulation, he argues that overly restrictive laws could infringe on valuable free expression and conflict with constitutional protections such as the First Amendment [8]. Similarly, Jacob R. Bourgault contends that existing speech exceptions may be too narrow to support broad regulation [9]. He calls for expansion of privacy rights as the main justification for deepfake regulation, he noted that while laws must address harm, they must not silence legitimate expression and should be carefully tailored.

Schuett evaluates the European Union's Artificial Intelligence Act using a risk-based framework that represents a global benchmark but suffers from inconsistent definitions that limit its effectiveness and overly broad categorization limits its practical effectiveness [10]. Finally, Fung and Etienne compare ethical principles across China and the EU. Their work suggests that cultural and philosophical differences shape regulatory priorities [11]. Together, those works provide valuable insights on jurisdiction-specific regulations with little focus on disinformation and free speech.

Therefore, this paper contributes to the existing debate by combining comparative legal analysis with cultural theory to show how national values influence regulatory choices. Moreover, this analysis provides a more comprehensive understanding of why fragmentation persists and explains why a hybrid governance model is the way forward.

4. REGULATORY PERSPECTIVES ON DEEPFAKES

4.1 Legal Perspective

A closer look at regulators worldwide shows different approaches. Some of them include sector-based (context of harm) or risk-assessment strategies, while others focus more on strict responsibility-based policies. The European Union has attempted to regulate deepfakes through existing frameworks such as the GDPR and the Digital Services Act [12], [13]. However, these frameworks offer only limited protection. Under the GDPR [12], for example, the regulation focuses on the identification and protection of individuals, but since deepfakes are synthetic content, they may involve features of several individuals or even mask attribution to a specific individual, which makes it challenging to apply this law effectively. As Schuett notes, this gap illustrates the limited capacity of some existing frameworks to address emerging AI technologies [10]. By contrast, the AI Act uses another approach, based on labeling manipulated content, which is supposed to contribute to "the development of an ecosystem of trust"[13]. While Schuett views the AI Act as a global benchmark, critics have highlighted inconsistencies in its definitions (Article 3(1) vs. Article 52) that creates uncertainty and undermines the legal effectiveness of addressing emerging challenges posed by deepfake [10], [14], [15]. Table 1 summarizes the findings.

Table 1. Different definitions in the Articles of the AI Act

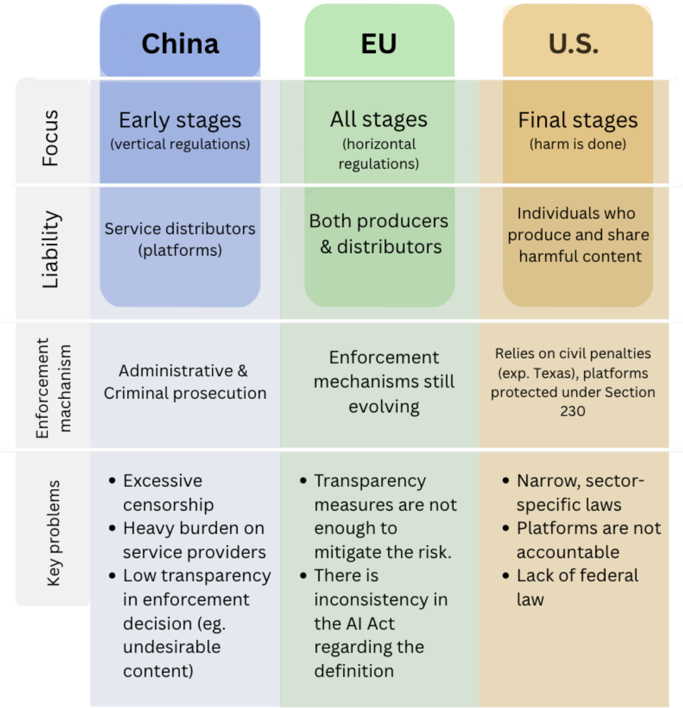
Article	Legal Requirement	Notable features
Art. 52 § 3(1)	Users of an AI system that generates or manipulates **text, audio or visual content** that would falsely … depictions of people appearing to … do things they did not … do, without **their consent** ('deep fake'), shall disclose….	● Includes text as a form of deepfake ● Mentions consent
Art. 3 § 1 (44d)	(44d) "deep fake" means manipulated or synthetic **audio, image or video content** that would falsely appear to be authentic or truthful, and which features depictions of persons appearing to say or do things they did not say or do, produced using AI techniques, including machine learning and deep learning	● Text not included as a form of deepfake ● Consent is not mentioned

Moreover, the AI framework is rooted on a trustworthy and transparent approach, but as was rightly pointed out by the European Commission that it won't be sufficient "to mitigate all risks associated with such applications" [16]. Therefore, effective governance must extend beyond disclosure to include mechanisms that mitigate the rapid spread and potential harms of synthetic media.

In the case of the United States, there is no federal law regulating deepfakes. It is fair to mention that there were a few legislative attempts (the Accountability Act of 2019 [17] and the formation of the Deepfake Provenance Task Force in 2021 [18]), but they were rejected by the committee and sent back for further revision. In practice, regulation is fragmented at the state level. Some states, like California (AB 602)[19], Texas(HB 3694)[20], Virginia (SB 18.2-386.2)[21] Maine (LD 132)[22], New York (S8631)[23], Colorado (HB 1147)[24], Florida (CS/HB 919)[25], and Washington (HB 5152) [26] have targeted laws addressing elections interference or non-conceptual pornography with Texas being the only state to classify the use of deepfakes in elections as a criminal offense [27]. Several proposed laws aimed at regulating deepfake technology are still struggling to gain adoption, including Virginia's HB2094 [29]. These fragmented attempts at regulation illustrate that there is no consensus on the appropriate legal consequences with the deepfake technology.

It is fair to argue that the U.S. approach remains largely sector-specific, with broader regulation constrained by constitutional limits. Scholars note that the First Amendment places significant barriers on regulating the body, as deepfakes are often treated as protected speech unless tied to fraud, defamation, or other narrow exceptions [7], [29]. This explains why states like California and Texas must demonstrate compelling justification to survive constitutional scrutiny. Similarly, the existing fragmentation of state-level laws illustrates the absence of a coherent national approach [30]. Moreover, platform liability remains blurred, as Section 230 of the Communications Decency Act shields online platforms from accountability for user-generated content—a protection that scholars argue paralyzes efforts to create proactive regulatory frameworks [31].

Unlike in the United States, China's regulatory approach focuses on deepfake technology service providers by holding them liable for not properly reviewing or labeling synthetic content and for failing to prevent the spread of information that contradicts law [32]. The Regulations on Deep Synthesis Management of Internet Information Services, which came into effect in 2023, adopts a significantly broader scope than traditional deepfake definitions. Instead of focusing solely on manipulated visual or audio content, the regulation focused on deep synthesis technology that includes areas such as immersive virtual reality and posture manipulation [33]. Strict rules imposed by Chinese authorities required providers verify user identity, label synthetic media and conduct security assessments to ensure traceability, all under the broader aim of maintaining social stability. While scholars acknowledge the regulation's breadth, they also caution that its ex-ante approach risks excessive censorship. Creemers notes that strict liability rules may encourage over-compliance, as providers could face criminal penalties for even minor oversights [32]. For instance, platforms like Weibo ban vaguely defined "undesirable" content, raising concerns about freedom of expression [34]. Deepfake regulation across the US, China and the EU are summarized in Figure 1.



	China	EU	U.S.
Focus	Early stages (vertical regulations)	All stages (horizontal regulations)	Final stages (harm is done)
Liability	Service distributors (platforms)	Both producers & distributors	Individuals who produce and share harmful content
Enforcement machanism	Administrative & Criminal prosecution	Enforcement mechanisms still evolving	Relies on civil penalties (exp. Texas), platforms protected under Section 230
Key problems	• Excessive censorship • Heavy burden on service providers • Low transparency in enforcement decision (eg. undesirable content)	• Transparency measures are not enough to mitigate the risk. • There is inconsistency in the AI Act regarding the definition	• Narrow, sector-specific laws • Platforms are not accountable • Lack of federal law

Fig 1. Deepfake Regulation: U.S., China, and EU

4.2 Cultural Perspective

To understand deepfake regulations across different jurisdictions the paper applies Geert Hofstede's Cultural Dimensions Theory. This framework helps to explain how national cultural values influence regulatory approaches, policy choices, and enforcement styles. Although the model based on six key dimensions, the presented analysis focuses on individualism - collectivism, power distance, uncertainty avoidance and long-term orientation, as they most directly shape regulatory approach [35].

- *Power Distance:* the extent to which members of a society are willing to accept and obey authority and tolerate unequal distributions of power. In countries like China, the Power Distance Index (PDI) is relatively high, which tends to accept hierarchical authority [43]. In particular, the regulatory approaches in China, rooted in Confucian philosophy, which emphasizes respect for hierarchy and the belief that the government acts in the best interest of its citizens—therefore, authority should not be questioned [11]. As a result, China's deepfake regulations are characterized by strict platform accountability, broad administrative discretion, and ex-ante control mechanisms.

In contrast, the pattern observed in lower power distance jurisdictions, such as the U.S. (PDI=40) and the EU (PDI=52, calculated as an average), aligns with lenient regulatory approaches that favor decentralization and procedural transparency in the use of deepfake algorithms [41], [42], [43]. These cultural norms reveal stronger preferences for lighter forms of interventions over strict ex-ante controls.

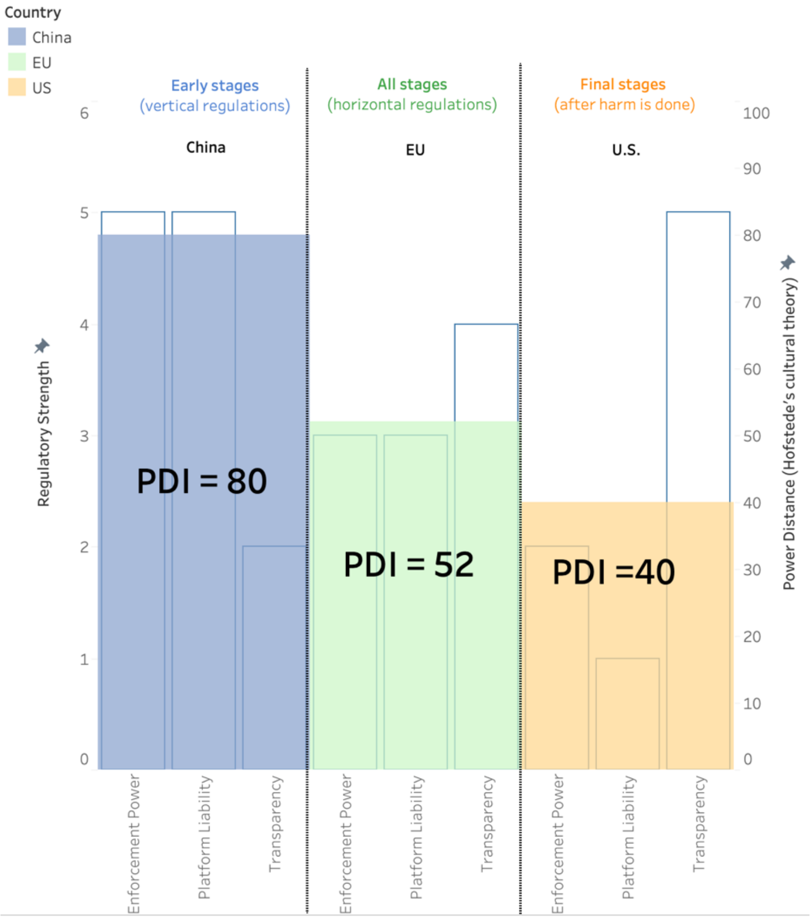


Figure 2. Regulatory Strength Across Jurisdictions with Cultural Overlay (Power Distance Index)

Figure 2 shows a clear alignment between PDI and regulatory design. China's high PDI (80) corresponds to its strong regulatory capacity across all three domains, which aligns with a governance model oriented toward centralized authority and proactive state intervention. The European Union shows moderate regulatory strength that aligns with its mid-level PDI (≈52) and risk-based regulatory philosophy. The last one, the United States, has the weakest regulatory capacity (PDI = 40), which highlights a cultural preference for autonomy and less regulation.

- *Individualism - Collectivism:* In China the sense of social responsibility and personal discipline motivates individuals to act for the collective good. In this framework, regulations are seen as a path to the "right way" to benefit society [11]. On the other hand, in the EU, people are more guided by a sense of individualism and rights-based approach, which has roots in the Enlightenment— when, as Kant put it, "man's emergence from his self-imposed immaturity" marked a shift toward intellectual independence and freedom from external authority [36]. Therefore, the legal framework created by the AI Act in the EU is more focused on protecting individuals from potential harms posed by technologies like deepfakes (risk-based approach). Similarly, the U.S. approach is also based on individualism, with a focus on prioritizing freedom of speech and expression—even at the risk of delayed accountability for the harms caused by deepfakes.

- *Uncertainty Avoidance and Long-Term Orientation*: According to Hofstede's classification [35], China is characterized as a country with a low Uncertainty Avoidance Index (UAI=30), which aligns with the greater openness towards adoption of new technologies. Still, the Chinese population tends to approach change with caution, demonstrating a stronger long-term orientation, as was observed by Shah et al. [38] and Khairullah [37]. Under Hofstede's model, low uncertainty avoidance would normally correspond to lower levels of regulatory strictness, however, China represents a clear exception, as shown in Figure 3. In China, strict regulation is driven more by high power distance, collectivist norms, and an interventionist governance model rather than by a low level of uncertainty avoidance [44].

In contrast, the United States (UAI = 46) shows a strong favor toward experimentation, rapid innovation, and reactive regulation (after harm has occurred). On the other hand, European countries have higher uncertainty avoidance index (UAI ≈ 72), which aligns with a more precautionary approach to AI governance. As a result, their horizontal regulatory safeguards are designed to protect citizens from potential technological harm at the early stages.

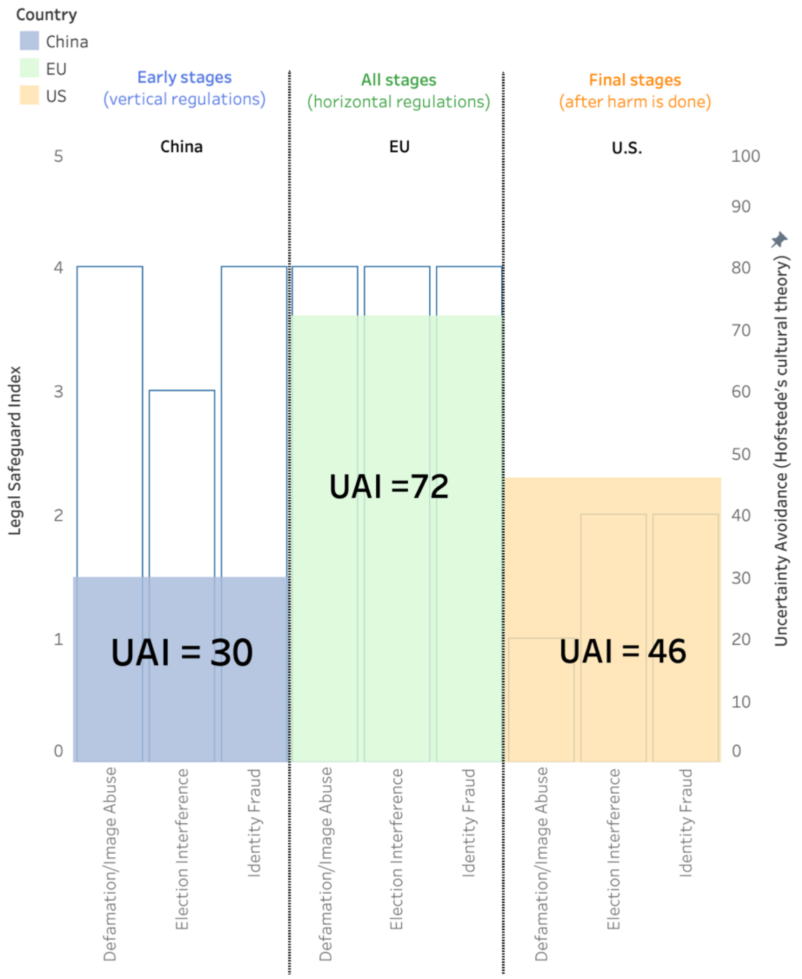


Figure 3. Cross-Cultural Comparison of Regulatory Responses to AI/Deepfake Harms with Cultural Overlay (Uncertainty Avoidance Index)

Figure 3 concludes the positioning of each regulatory model against their respective Uncertainty Avoidance Index. While this index helps explain Western regulatory patterns, China's model reflects a politically driven logic of social stability rather than cultural uncertainty avoidance, which makes it an outlier within Hofstede's framework.

The broader findings indicate that cultural values shape not only attitudes toward risk perception but also determine the regulatory choices in response to innovations.

5. DISCUSSION AND RECOMMENDATIONS

The analysis concluded that the regulation of deepfake technology is very fragmented. This, in turn, creates regulatory arbitrage where malicious actors exploit weakness in jurisdictions and undermines the ability to respond to cross-border harms. For example, the 2023 Pentagon deepfake incident, which briefly triggered stock market volatility, illustrates how gaps in the U.S. law allow harmful content to spread before regulators can respond [39]. Similarly, the EU's reliance on labeling cannot prevent the viral circulation of manipulated media, while China's expansive regulations risk suppressing freedom of expression in the name of social order. Moreover, cultural values cannot be overlooked, as they set the boundaries of what legal solutions are politically and socially possible. In collectivist systems such as China, regulations are framed as a duty to preserve stability, in individualist systems such as the U.S. and the EU, regulation is bounded by speech rights and individual freedoms. This paper contributes to the broader debate by showing that without integrating cultural perspectives, legal comparisons alone cannot fully explain fragmentation or point toward viable solutions. Together, these findings suggest that harmonization cannot mean identical laws. Instead, convergence requires agreement on minimum safeguards. This may include a universally recognized definition. Without clarity in definition, enforcement will remain inconsistent across jurisdictions [10], [15]. Moreover, regulators should combine ex-ante measures with ex-post penalties for platform providers. This balances freedom of expression with accountability and responds to the gaps identified in the U.S. and the EU frameworks [7], [31]. Finally, regulators should ensure that cultural differences are acknowledged but not allowed to justify regulatory gaps. Instead, convergence should occur around baseline safeguards [11]. For example, in drafting frameworks, collectivist systems may emphasize stability while individualist systems prioritize right.

6. CONCLUSION

This paper has argued that the difficulty of regulating deepfakes lies not only in the novelty of the technology but also in the fragmentation of legal and cultural frameworks across jurisdictions. The comparative analysis has shown how different cultural orientations shape distinct regulatory trajectories. The regulatory approaches range from reactive (post-harm) models to precautionary horizontal safeguards and ex-ante, state-driven controls. These differences show that regulatory choices are not only technical control measures but also shaped by cultural-social contexts. In other words, cultural orientation sets the outer boundaries of legal frameworks and defines which strategies will be feasible. The findings suggest that the path toward effective governance of deepfakes will require agreement on a small set of minimum safeguards. In particular, shared definitions of synthetic media, hybrid liability frameworks (with defined responsibilities between platforms and users), and transparency obligations. This approach respects national differences and at the same time establishes common protections against the most consequential harms posed by deepfakes.

There is a need for further analysis of how these minimum safeguards can be implemented within the cross-border contexts where deepfake content circulates rapidly. For this purpose, more empirical studies are needed to analyze the effectiveness of the proposed method, as well as to assess the impact of disclosure mechanisms on user behavior. Additionally, regulators should consider integrating tools such as authenticated media pipelines, watermark- standards, and international cooperative frameworks. This direction will help refine regulatory strategies and ensure that governance models remain adaptive to future technological development.

7. REFERENCES

[1] Tripathi, S., Augustin, A.I., Dunlop, A., Sukumaran, R., Dheer, S., Zavalny, A., Haslam, O., Austin, T., Donchez, J., Tripathi, P.K., and Kim, E. 2022. Recent advances and application of generative adversarial networks in drug discovery, development, and targeting. Artificial Intelligence in the Life Sciences. 2(Dec.2022),1–21. https://doi.org/10.1016/j.ailsci.2022.100035

[2] McCosker, A. 2022. Making sense of deepfakes: Socializing AI and building data literacy on GitHub and YouTube. New Media & Society. 26, 5 (May 2022),2786–2803. https://doi.org/10.1177/14614448221102214

[3] Balkin, J. 2018. Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. UC Davis Law Review. 51, 3 (2018), 1149–1210.

[4] Schwartz, O. 2018. You thought fake news was bad? Deep fakes are where truth goes to die. The Guardian. (Nov. 12, 2018). Retrieved May 4, 2025 from https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth

[5] Vaccari, C. and Chadwick, A. 2020. 'Deepfakes' are here. These deceptive videos erode trust in all news media. The Washington Post. (May 24, 2020). Retrieved May 4, 2025 from https://www.washingtonpost.com/opinions/2020/05/24/deepfakes-deceptive-videos-erode-trust-news-media/

[6] Smith, B. 2023. Advancing AI governance in Europe and internationally. Microsoft Blog. (Jun. 2023). Retrieved May 4,2025from https://blogs.microsoft.com

[7] Citron, D.K. and Chesney, R. 2019. Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review. 107, 6 (2019), 1753–1819.

[8] Wilkerson, L. 2021. Still waters run deep(fakes): The rising concerns of "deepfake" technology and its influence on democracy and the First Amendment. Missouri Law Review. 86, 1 (2021). Available at: https://scholarship.law.missouri.edu/mlr/vol86/iss1/12

[9] Bourgault, J.R. 2021. Free speech and synthetic lies: Deepfakes, synthetic media, and the First Amendment. Stanford Journal of International Law & Policy. 12, 1 (2021), 45–78.

[10] Schuett, J. 2023. Risk management in the Artificial Intelligence Act. European Journal of Risk Regulation. 15, 2 (Jun. 2023), 367–385. https://doi.org/10.1017/err.2023.12

[11] Fung, P. and Etienne, H. 2021. Confucius, Cyberpunk and Mr. Science: Comparing AI ethics between China and the EU. Cornell University Preprint. (Nov. 2021). Available at SSRN: https://ssrn.com/abstract=3962929

[12] GDPR. 2025. What is considered personal data under the EU GDPR? Retrieved May 1, 2025 from https://gdpr.eu/eu-gdpr-personal-data/

[13] EUR-Lex. 2021. Document 52021PC0206. Retrieved May 1, 2025 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

[14] Veale, M. and Zuiderveen Borgesius, F. 2021. Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International. 22, 4 (2021), 97–112. Available at SSRN: https://ssrn.com/abstract=3896852

[15] Edwards, L. 2022. Regulating AI in Europe: Four problems and four solutions. Ada Lovelace Institute Expert Opinion. (Mar. 1, 2022). Available at SSRN: https://ssrn.com/abstract=5026691

[16] Access Now. 2021. Access Now's submission to the European Commission's adoption consultation on the Artificial Intelligence Act. (Aug. 2021). Retrieved May 1, 2025 from https://www.accessnow.org/wp-content/uploads/2021/08/Submission-to-the-European-Commissions-Consultation-on-the-Artificial-Intelligence-Act.pdf

[17] U.S. Congress. 2019. H.R.3230 – DEEP FAKES Accountability Act. Retrieved May 2, 2025 from https://www.congress.gov/bill/116th-congress/house-bill/3230

[18] U.S. Congress. 2021. S.2559 – Deepfake Task Force Act. Retrieved May 2, 2025 from https://www.congress.gov/bill/117th-congress/senate-bill/2559

[19] California Legislative Information. 2019. Assembly Bill No. 602. Retrieved May 2, 2025 from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602

[20] Capitol Texas. 2025. H.B. No. 3694. Retrieved May 3, 2025 from https://capitol.texas.gov/tlodocs/89R/billtext/html/HB03694I.htm

[21] Virginia Law. 2025. § 18.2-386.2. Unlawful dissemination or sale of images of another; penalty. Retrieved May 3, 2025 from https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/

[22] Maine Legislature. 2023. An Act Regarding Artificial Intelligence in Campaign Advertising. Retrieved May 2, 2025 from

https://legislature.maine.gov/legis/bills/getMSWORD.asp?paper=HP1125&item=1&snum=132

[23] State of New York, Senate. 2023. House Bill 1042–A. Retrieved May 3, 2025 from https://legislation.nysenate.gov/pdf/bills/2023/S1042A

[24] General Assembly, State of Colorado. 2024. House Bill 24-1147. Retrieved May 2, 2025 from https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_1147_01.pdf

[25] Florida House of Representatives. 2024. CS/HB 919 – Artificial Intelligence Use in Political Advertising. (Mar. 2024). Retrieved May 2, 2025 from https://www.flsenate.gov/Session/Bill/2024/919/Analyses/h0919z1.EEG.PDF

[26] State of Washington. 2023. Senate Bill 5152. Retrieved May 2, 2025 from https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Senate%20Passed%20Legislature/5152-S.PL.pdf

[27] Capitol Texas. 2019. S.B. No. 751 – An act creating a criminal offense for fabricating a deceptive video with intent to influence an election. (Mar. 2019). Retrieved May 2, 2025 from https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751S.htm

[28] Virginia State Legislative System. 2025. HB2094 – High-risk artificial intelligence; definitions, development, deployment, and use, civil penalties. Retrieved May 2, 2025 from https://lis.virginia.gov/bill-details/20251/HB2094

[29] Volokh, E. 2019. Deepfakes, free speech, and the law. University of Chicago Law Review Online. 82 (2019).

[30] Douek, E. 2021. Deep fakes: A looming crisis for national security, democracy, and privacy? Harvard Journal of Law & Technology. 34 (2021).

[31] Keller, D. 2019. Who do you sue? State and platform hybrid power over online speech. Hoover Institution Aegis Series Paper No. 1907. (2019).

[32] Creemers, R. and Webster, G. 2022. Translation: Internet Information Service Deep Synthesis Management Provisions (Draft for Comment). Stanford University. (Feb. 2022).

[33] Sheehan, M. 2023. China's AI regulations and how they get made. Carnegie Endowment for International Peace. (Jul. 2023).

[34] Wakabayashi, D. and Fu, C. 2024. China's censorship dragnet targets critics of the economy. The New York Times. (Jan. 31, 2024).

[35] Hofstede, G. 2011. Dimensionalizing cultures: The Hofstede model in context. Online Readings in Psychology and Culture. 2, 1 (Dec. 2011), 3–26. https://doi.org/10.9707/2307-0919.1014

[36] UCSB. 2025. What is Enlightenment? Retrieved May 3, 2025 from https://donelan.faculty.writing.ucsb.edu/enlight.html

[37] Khairullah, D.H.Z. and Khairullah, Z.Y. 2013. Cultural values and decision-making in China. International Journal of Business, Humanities and Technology. 3, 2 (Feb. 2013).

[38] Shah, R., Gao, Z., and Mittal, H. 2015. Conclusions and thoughts about the future: The United States, China, and India. In Handbook of Innovation, Entrepreneurship, and the Economy in the US, China, and India. Historical Perspectives and Future Trends. Elsevier Inc., 333–350.

[39] The Guardian. 2023. AI-generated image of Pentagon explosion briefly causes stock market dip. (May 22, 2023). Retrieved May 4, 2025 from https://www.theguardian.com/technology/2023/may/22/ai-generated-image-pentagon-explosion-stock-market

[40] Cyberspace Administration of China. 2022. Provisions on the Administration of Deep Synthesis Internet Information Services. Promulgated Dec. 11, 2022, effective Jan. 10, 2023. Available at: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm

[41] National Institute of Standards and Technology (NIST). 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce, Gaithersburg, MD. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[42] European Commission. 2024. Artificial Intelligence Act (EU 2024/1689). Official Journal of the European Union, L, 2024, 1689. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[43] Hofstede Insights. 2015. Dimension data matrix. Retrieved from https://geerthofstede.com/research-and-vsm/dimension-data-matrix/

[44] Xue, Z., & Lu, J. (2018). A cross-cultural comparative analysis of Sino-American family conflicts management. Theory and Practice in Language Studies, Volume(8), pp. 516-521, https://www.academypublication.com/issues2/tpls/vol08/05/09.pdf