Archives of Current Research International

Volume 24, Issue 12, Page 52-74, 2024; Article no.ACRI.127855
ISSN: 2454-7077

Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry

Jumai Adedoja Fabuyi [a++*], Oluwaseun Oladeji Olaniyi [b#], Omobolaji Olufunmilayo Olateju [c†], Nsidibe Taiwo Aideyan [d‡], Oluwatosin Selesi-Aina [d#] and Folashade Gloria Olaniyi [e^]

[a] University of Illinois Urbana Champaign, 901 West Illinois Street, Urbana, IL 61801, United States of America.
[b] University of the Cumberlands, 104 Maple Drive, Williamsburg, KY 40769, United States of America.
[c] University of Ibadan, Oduduwa Road, Ibadan, Oyo State, Nigeria.
[d] University of Lagos, University Road Lagos Mainland Akoka, Yaba, Lagos, Nigeria.
[e] University of the People, 595 E Colorado Blvd Suite 623, Pasadena, CA 91101, United States of America.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/acri/2024/v24i12997

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/127855

Original Research Article

Received: 04/10/2024
Accepted: 08/12/2024
Published: 13/12/2024

[++] Privacy and Artificial Intelligence Governance Researcher;
[#] Information Technology Researcher;
[†] Agricultural Technology Researcher;
[‡] Law and Information Governance Researcher;
[^] Cyber Security and Data Expert;
**Corresponding author: Email: adedoja.jay@gmail.com;*

Cite as: *Fabuyi, Jumai Adedoja, Oluwaseun Oladeji Olaniyi, Omobolaji Olufunmilayo Olateju, Nsidibe Taiwo Aideyan, Oluwatosin Selesi-Aina, and Folashade Gloria Olaniyi. 2024. "Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry". Archives of Current Research International 24 (12):52-74. https://doi.org/10.9734/acri/2024/v24i12997.*

ABSTRACT

This study investigates the impact of region-specific regulatory approaches on the use of deepfake technology within the entertainment industry, focusing on the United States, European Union, and China. Using data from the World Bank and OECD on regulatory quality and rule of law, the study employs a quantitative methodology that includes multivariate regression, chi-square tests, and logistic regression. Key findings reveal that while U.S. and EU regulations prioritize transparency and individual rights, China adopts a state-centered approach emphasizing social stability. Verification protocols in traditional media significantly enhance public trust ($p < 0.001$), while compliance costs support economic stability but slightly diminish trust. Social media platforms like YouTube and TikTok demonstrate robust content moderation policies, aligning more closely with regulatory expectations than Facebook and Twitter. The research highlights the influence of public opinion on regulatory effectiveness, noting its critical role in balancing innovation, ethical responsibility, and public trust. By examining the interplay of cultural, ethical, and economic factors, this study underscores the importance of harmonizing international regulations to mitigate the risks associated with deepfake technology. Recommendations include strengthening verification protocols, enhancing public digital literacy, and fostering global regulatory cooperation to create a framework that promotes innovation while safeguarding ethical standards. The findings offer valuable insights for policymakers, content creators, and media platforms navigating the complexities of AI-driven content in the digital age.

Keywords: Deepfake regulation; artificial intelligence; entertainment industry; public trust; compliance costs; multivariate regression.

1. INTRODUCTION

The rapid rise of artificial intelligence (AI), especially through the advent of deepfake media, has introduced both new opportunities and substantial challenges, particularly within the entertainment sector. Initially celebrated for enhancing creative possibilities, deepfake technology has since come under scrutiny for its ability to produce highly realistic representations of individuals, often resulting to potential misuse and deception (Montasari, 2024). This technology employs deep learning to modify or create digital media, such as faces, voices, and gestures, which results in synthetic content that closely mimics reality. Gregory (2021) argues that deepfakes' capacity to blur the line between genuine and manipulated media has made the technology a focal point in a complex regulatory environment, where maintaining a balance between creative freedom and protections against misuse is essential. This study addresses a critical gap in understanding the implications of deepfake regulations on content creation within the entertainment industry. By focusing on the regulatory approaches of the United States, European Union, and China, the research offers a comparative analysis of how cultural, ethical, and economic factors shape policy development. Efforts to regulate deepfake technology have led social media, streaming platforms, and traditional media outlets to implement policies aimed at minimizing harm. Major platforms like Facebook, Twitter, and TikTok have introduced measures to detect and remove harmful deepfake content in response to both national and international pressures (Wakefield, 2021). In the U.S., these platforms are guided by the Malicious Deep Fake Prohibition Act, which requires the removal of maliciously intended media. Streaming services such as YouTube have adopted similar policies, deterring deceptive deepfakes through monetization restrictions by penalizing or demonetizing violative content. Traditional media, dedicated to maintaining journalistic integrity, has raised editorial standards, incorporating verification protocols to preserve societal trust. Additionally, practices like disclosure and labelling help differentiate real content from AI-generated media, allowing audiences to better assess the accuracy of the information (Knott et al., 2024).

Universally, responses to deepfakes highlight a developing regulatory landscape shaped by varied cultural, social, and economic influences. The EU's General Data Protection Regulation (GDPR), though not explicitly targeting deepfakes, offers privacy protections that stresses the ethical need for consent when using an individual's likeness in AI-generated media (Hoofnagle et al., 2019). These findings are vital for guiding international regulatory

harmonization, fostering public trust, and promoting ethical standards in the use of AI-driven technologies. By highlighting the interplay between compliance practices, public trust, and economic stability, the research underscores the transformative potential of well-structured regulations in fostering a responsible and sustainable entertainment industry. The upcoming Digital Services Act builds on this by mandating that major platforms monitor and remove harmful synthetic content, prioritizing transparency and user safety (Eurojust, 2022). China's regulatory strategy focuses on social stability, requiring clear labelling of deepfake content to prevent public unrest and aligning with a state-centred model of information oversight. In contrast, the United States adopts a more decentralized approach, using state-specific regulations like California's AB602 and AB730 to combat malicious deepfake use, yet lacking a cohesive federal policy (Metwally, 2019).

In the entertainment industry, creators face a regulatory environment that demands strict adherence to complex compliance standards and ethical responsibilities. Legal system on intellectual property, data protection, and authorization are increasingly limiting how deepfake technology can be used. Noti-Victor (2024) suggests that creators are now expected to ensure transparency, obtain permissions for synthetic representations, and disclose any AI-generated elements in their work as a means of maintaining public trust, and while these regulations pose creative and logistical challenges, they promote responsible content production, helping to preserve public trust and prevent misuse. Ethical issues often emerge, especially when deepfakes are used without consent, such as in synthetic pornography. In response, countries like South Korea and the United Kingdom have introduced laws to protect individual rights and dignity, highlighting the need for regulatory measures to address these ethical concerns (Mania, 2022). All platforms and creators must use deepfake technology responsibly, ensuring it fosters creative innovation rather than deception. Traditional media, grounded in journalistic principles, has adopted stricter verification and disclosure measures to prevent misinformation, preserving credibility in the face of growing synthetic media. Legal repercussions for the malicious distribution of deepfakes further emphasize the importance of regulatory compliance and the need for responsible use (Montasari, 2024).

Recent legislative developments highlight the social, economic, and ethical aspects of regulating deepfakes. Allyn (2024) points out that California's AI Safety Bill (SB 1047), which has gained significant support in Hollywood, reflects the entertainment industry's recognition of the risks posed by unregulated AI, including deepfakes; the American Civil Liberties Union (ACLU) has raised concerns about overly restrictive deepfake laws, calling for a balanced approach that protects free speech while preventing harm to individuals. Legal disputes, such as Voicify's case over AI-generated music, emphasize the challenges of preserving intellectual property rights in the age of synthetic media. These cases highlight the urgent need for carefully crafted regulatory frameworks that foster innovation while maintaining ethical standards and legal protections (ACLU, 2022). Public perception of deepfakes has evolved, reflecting a growing awareness of their potential risks. Studies show a dramatic surge in deepfake videos online, with an estimated 550% increase since 2019, and approximately 96% of these involve non-consensual pornographic content targeting women (Ramirez & Andrada, 2024; Evans, 2023). This reality highlights the urgent need for regulatory action as public concern intensifies. Surveys reveal that only 30% of individuals are confident in identifying manipulated media, while around 77% support stronger legal measures to prevent misuse (Weikmann et al., 2024; Evans, 2023).

As deepfake technology continues to evolve, ongoing dialogue among policymakers, technology companies, content creators, and the public will be crucial in developing frameworks that protect creative freedoms while preventing misuse. This discussion highlights the need to balance the transformative potential of deepfakes with ethical oversight, ensuring that AI-driven innovations in content creation strengthen public trust and protect individual rights (Al-kfairy et al., 2024a). This study seeks to examine the regulatory landscape surrounding Deepfake AI usage in content creation within the entertainment industry, exploring the impact of these regulations across social media, streaming platforms, mass media, and their adoption in diverse international contexts, with the following objectives:

1. Assesses the global regulatory approaches to deepfakes, comparing the approaches of the United States, the European Union, and China, examining

the specific laws, policies, industry standards, and their effectiveness in curbing the misuse of synthetic media across international borders.
2. Analyzes the specific regulatory frameworks governing deepfake technology on social media and streaming platforms, including their scope, enforcement, and implications for content creators in terms of challenges faced, opportunities created, and ethical considerations.
3. Investigates the compliance requirements and limitations imposed by deepfake regulations on traditional mass media outlets, with particular attention to journalistic integrity and public trust.
4. Evaluates the broader social, ethical, and economic implications of deepfake regulations on the entertainment industry, particularly regarding creative freedom, public awareness, and industry adaptation.
5. Proposes recommendations for future policy development and industry best practices to balance the potential benefits of deepfake technology with the need to mitigate its risks and harms.

2. LITERATURE REVIEW

As deepfake technology rapidly advances, the United States, European Union, and China have each introduced regulatory frameworks tailored to their unique socio-political, economic, and cultural contexts. In the U.S., regulation has primarily developed at the state level, with California leading efforts through legislation like AB602 and AB730 (Metwally, 2019). As stated by Birrer and Just (2024), these laws specifically target the non-consensual and politically manipulative use of deepfakes, including prohibitions on unauthorized media in pornography and the spread of misleading political content (Sobel, 2024; Adigwe et al., 2024). Nevertheless, without a cohesive federal framework, state-level initiatives have limitations in effectively addressing deepfake misuse nationwide (Chawki, 2024; Akinola et al., 2024). As a result, federal proposals like the DEEPFAKES Accountability Act aim to establish uniform protections emphasizing individual rights, especially against identity misrepresentation and non-consensual media use, as Murray (2024) explains. Additionally, the entertainment industry has actively contributed to this regulatory push, with bipartisan initiatives like the NO FAKES Act, which is supported by prominent artists, and California's AI Safety Bill (SB 1047), both addressing exploitation risks associated with AI in entertainment (Maddaus, 2024; Alao et al., 2024).

Conversely, the European Union has taken a more centralized and comprehensive approach to regulation, embedding deepfake governance within its broader policies on AI and digital content (Nanni et al., 2024; Arigbabu et al., 2024). The EU's Artificial Intelligence Act and Digital Services Act (DSA) impose strict transparency requirements, mandating clear labeling of synthetic media to ensure that viewers can identify its artificial origin (Krack et al., 2022; Arigbabu, Olaniyi, Adigwe, et al., 2024). The European Commission (2021) suggests that these regulations are consistent with the EU's established data privacy system, and is strengthened by the General Data Protection Regulation (GDPR), which requires deepfake creators to obtain consent for likeness use, thereby enhancing privacy protections and discouraging unauthorized media manipulation. However, some critics argue that these strict policies could stifle creativity in the entertainment industry by imposing substantial compliance burdens on content creators (Gavrilova et al., 2022; Deng & Chen, 2023; Asonze et al., 2024).

China's regulatory approach, spearheaded by the Cyberspace Administration's Deep Synthesis Regulation, emphasizes social stability and control over misinformation. As Hemrajani (2023) notes, this regulation requires clear labeling of synthetic media and restricts content creation to enforce accountability, highlighting China's preference for a centralized, state-managed digital framework. While this approach seeks to limit the spread of false information, it significantly restricts creative freedom, preventing Chinese content creators from fully exploring the artistic possibilities of deepfake technology. While China's model represents a government-centered regulatory strategy that prioritizes social order over individual autonomy, it, contrasts with the more individual-focused approaches seen in the U.S. and EU (Jin & Shao, 2024; Gbadebo et al., 2024). These regulatory strategies highlight various national priorities in managing deepfake technology: the U.S. emphasizes criminalization and individual rights, the EU prioritizes transparency and data privacy, and China focuses on social control. As deepfake technology continues to evolve, international cooperation may be essential for

regulatory alignment, helping to address its cross-border impacts and encourage responsible use (Jin & Shao, 2024; Braine, 2020; Matheus et al., 2021; Joeaneke et al., 2024).

2.1 Deepfake Regulations Across Social Media and Streaming Platforms

Social media and streaming platforms' regulatory approaches to deepfake content illustrate the intricate balance between content moderation, ethical accountability, and freedom of expression. In accordance with Malik, Surbhi, and Roy (2024), platforms like Facebook, Twitter, and TikTok have enacted policies aimed at addressing harmful deepfakes, requiring either removal or labelling to alert users to manipulated media. Facebook's policy, for example, bans synthetic media specifically designed to mislead the public, with a focus on politically sensitive content. Similarly, Twitter uses labels to flag potentially misleading media, while TikTok applies explicit labels to AI-generated content to promote transparency in user interactions (Vaccari & Chadwick, 2020; TikTok, 2019; Joeaneke et al., 2024). However, Shao et al. (2022) argues that the swift advancement of AI complicates detection, as increasingly sophisticated algorithms create highly realistic modifications that current AI tools struggle to accurately identify.

These detection challenges are further complicated by ongoing discussions about the implications for free speech (Prakash et al., 2021; Yang et al., 2022; John-Otumu et al., 2024); the American Civil Liberties Union (ACLU) contends that strict deepfake regulations could violate First Amendment rights, especially when synthetic media is used for satire, parody, or commentary (ACLU, 2022). According to Al-kfairy et al. (2024b), this viewpoint emphasizes the importance of balancing protection against misinformation with the preservation of creative expression. Scholars supporting the ACLU's position suggest that platforms should carefully balance harm prevention with maintaining diverse voices in digital spaces, to avoid censoring lawful content (Baik & Sridharan, 2023; ACLU, 2022; Joseph, 2024). Additionally, these regulations impose ethical responsibilities on content creators, who must navigate platform guidelines to avoid unintended penalties. These platforms are increasingly urging creators to disclose their use of AI, a practice that, according to Gao et al. (2023), promotes transparency but may also decrease user engagement due to caution surrounding synthetic media.

Streaming platforms like YouTube adhere to similar regulatory frameworks, with community guidelines that explicitly ban content intended to mislead or harm viewers, especially in political and financial contexts. As noted by Moreno (2024), YouTube utilizes AI systems to detect and flag deepfake content, emphasizing its commitment to responsible media consumption. Additionally, monetization policies serve as a deterrent, as content that violates deepfake guidelines risks demonetization or exclusion from ad revenue, thus encouraging creators to follow ethical standards (Tan, 2022; Malik et al., 2024). However, Knott et al. (2024) points out that relying on automated detection raises concerns about accuracy, as these systems sometimes produce false positives, flagging legitimate content, which highlights the need for ongoing improvements in moderation tools to guarantee accurate and equitable content management.

Together, these regulatory initiatives demonstrate the adaptive strategies that social media and streaming platforms use to manage deepfake risks (Montasari, 2024; Ogungbemi et al., 2024). According to Park and Rohatgi (2024), while these platforms aim to control harmful content, maintaining a delicate balance between regulation, ethical responsibility, and freedom of expression is crucial. All these challenges emphasize the need for strong, flexible frameworks to address the impact of deepfake technology, particularly as authenticity and transparency become increasingly important in the digital landscape.

2.2 Deepfake Regulations in Mass Media and Traditional Journalism

The rise of deepfake technology has posed significant challenges for mass media and traditional journalism, leading to the implementation of stricter verification protocols and reinforced editorial standards to maintain public trust. News organizations are increasingly utilizing a blend of manual and automated methods to verify content authenticity, particularly in sensitive areas like political reporting (Thomson et al., 2020; Okon et al., 2024). According to Spyropoulos et al. (2023), digital forensics tools, which analyzes metadata and identify visual inconsistencies, are now often paired with human oversight to improve accuracy and reduce misinformation; these verification processes are deemed vital to journalistic integrity, ensuring that audiences receive trustworthy information amid growing risks of

digital manipulation (Sharma & Rout, 2024; Olabanji et al., 2024). Transparency and disclosure practices are crucial for promoting informed media consumption. Garon (2023) argues that many media organizations require clear labeling of synthetic media, particularly in historical or documentary contexts where deepfake technology might reconstruct past events or present hypothetical scenarios. This practice helps viewers distinguish between genuine and manipulated content, fostering more informed judgments about authenticity (Thomas, 2024; Oladoyinbo et al., 2024). Supporting this push for transparency, the European Union's AI Act has formalized labeling requirements, however, Allan et al. (2021) notes that achieving global consistency in these standards remains difficult due to differing regulatory landscapes, which affect enforcement.

The Voicify case, a legal dispute between a UK-based start-up and the British Phonographic Industry (BPI), highlights the intellectual property challenges posed by deepfake technology (Business Matters, 2024; Olaniyi, 2024). Voicify's AI-generated music, which mimics the voices of famous artists, has sparked debate over whether existing copyright laws are adequate for regulating AI-driven content creation (Business Matters, 2024; Olaniyi, 2024; Thomson et al., 2020). Cooke (2024) argues that while Voicify defends its technology as a form of creative expression, the BPI contends it violates artists' rights and calls for regulatory action against unauthorized replication of likenesses. This case reflects broader legal and ethical issues, emphasizing the need for systems that balance innovation with intellectual property protections in AI (Abdallah & Salah, 2023; Olaniyi et al., 2024).

Deepfake regulations also impact journalistic practices, prompting organizations to re-evaluate standards for source verification and ethical reporting (Farouk & Fahmi, 2024; Olaniyi et al., 2023). While disclosure protocols improve accuracy, they can also restrict creative freedom, especially when AI is used responsibly in contexts like historical reconstructions or narrative illustrations (Cheong et al., 2024; Olaniyi, Omogoroye, et al., 2024). de-Lima-Santos et al. (2024) observes that although these limitations may seem restrictive, regulatory bodies in both the U.S. and EU emphasize the importance of transparency in enhancing public awareness, allowing a clearer understanding of AI's role in media without undermining journalistic integrity. The emergence of deepfake technology requires a rethinking of journalistic standards, prompting media organizations to implement thorough verification and transparency protocols (Kothari & Cruikshank, 2021; Olaniyi, Ugonnia, et al., 2024). The Voicify case illustrates the conflict between creative expression and intellectual property rights, emphasizing the legal and ethical implications of synthetic media (Abdallah & Salah, 2023; Olateju et al., 2024).

2.3 Broader Social, Ethical, and Economic Implications of Deepfake Regulations

The rise of deepfake technology has sparked significant social, ethical, and economic concerns, requiring comprehensive supervisory approaches to preserve public trust, protect individual rights, and manage industry growth. Farouk and Fahmi (2024) contend that socially, deepfake regulations play a critical role in shaping public perceptions of media authenticity. Research shows that only about 30% of individuals are confident in distinguishing real content from manipulated media, creating challenges for media organizations that rely on audience trust (Weikmann et al., 2024; Luo et al., 2020; Olateju, Okon, Olaniyi, et al., 2024), and as a result, regulations requiring the disclosure and labeling of synthetic media aim to address this trust deficit. However, without consistent enforcement, these measures may fall short of restoring public confidence, as audiences remain wary of the potential for digital manipulation (George & George, 2023; Salami et al., 2024). To tackle this skepticism, public education campaigns have become crucial tools for improving media literacy (Dame Adjin-Tettey, 2022; Samuel-Okon et al., 2024). Farouk and Fahmi (2024) propose that awareness initiatives, such as media literacy programs focused on deepfake technology, can enhance detection accuracy by over 40%, enabling individuals to make informed decisions about content authenticity, while DiGiacomo et al. (2023) argues that while these programs bolster digital resilience, policymakers contend that education alone cannot fully counter the rapid evolution of synthetic media. Therefore, a balanced approach that combines regulation with public awareness is recommended to promote responsible media consumption.

Ethically, deepfakes raise complex issues surrounding privacy and consent; the illegal use of an individual's likeness in synthetic media can violate privacy, damage reputations, and lead to potential legal disputes. Florea and Esteves

(2023) argue that consent should be a fundamental requirement, in line with principles of individual autonomy, as supported by regulations like the European Union's GDPR, which mandates consent for the use of personal data in synthetic content. However, some caution that strict approval requirements may hinder creative expression, especially when deepfake technology is used for satire or artistic purposes. This is a conflictual issue, because it emphasized the need to balance creative freedom with ethical responsibility, as content creators navigate the fine line between innovation and respecting personal rights (Thongmeensuk, 2024; Samuel-Okon, Olateju, et al., 2024).

Economically, deepfake technology has presented both opportunities and difficulties, transforming market dynamics within the media and entertainment industries. The rising demand for synthetic media has drawn significant investment, with projections indicating that the AI-driven content market could surpass $79 million by 2024 (Davis, 2024). Alcántara et al. (2024) notes that while deepfakes hold commercial potential in advertising, visual effects, and personalized content, regulatory restrictions on platforms like YouTube limit monetization, as non-compliant content faces demonetization or removal. As a result, creators must strike a balance between profitability and adherence to ethical principles, shaping content production in a digital economy increasingly shaped by platform policies. The financial dangers associated with deepfakes also encompass insurance and liability concerns, as companies face claims related to privacy violations and defamation (Delfino, 2024; Selesi-Aina et al., 2024). This has led to the development of specialized insurance policies for AI-related risks; however, the high costs of these policies may make it difficult for smaller creators to acquire coverage, highlighting disparities in the industry's ability to manage deepfake risks. These social, ethical, and economic factors emphasize the interconnectedness of deepfake regulation, highlighting the need for flexible policies to address the evolving challenges posed by synthetic media (Farouk & Fahmi, 2024).

2.4 Future Directions and Recommendations for Deepfake Policy Development

Future policy development on deepfake technology should emphasize international collaboration to tackle the global challenges posed by synthetic media. Research indicates that discrepancies between national regulations hinder effective enforcement on international platforms, as content frequently originates from multiple jurisdictions (Jenny, 2021; Chapdelaine & McLeod Rogers, 2021; Haggart & Keller, 2021). A unified international structure could foster accountability by establishing consistent disclosure practices and shared compliance standards to reduce the spread of harmful deepfakes. Experts suggest that cooperation among major economies is essential to effectively limit misuse, while also respecting regional differences in media freedom, thus creating a more integrated regulatory approach (Huang et al., 2024; Nguyen & Tran, 2023; Wolniak & Steculа, 2024).

Setting ethical standards for content creators is crucial to promote responsible use of deepfake technology, Pickering (2021) argues that protocols focusing on transparency and informed consent would help creators navigate ethical dilemmas while adhering to platform policies designed to uphold public trust. Clear disclosure of AI-generated content is essential for minimizing deception, raising audience awareness, and clarifying the responsibilities of creators in managing the potential risks associated with synthetic media. Policymakers must strike a balance between fostering innovation and ensuring public safety by implementing flexible regulations that adapt to AI advancements without stifling creativity. Lescrauwaet et al. (2022) contends that an adaptive regulatory approach, shaped by cooperation among policymakers, industry experts, and civil society, will facilitate both ethical and technological progress within responsible limits. By adopting a multi-stakeholder framework, regulatory standards can effectively address the complex challenges posed by deepfake technology, promoting innovation while ensuring accountability. This flexible, collaborative approach highlights the need for sustainable deepfake regulation, creating a digital environment that upholds individual rights and ethical standards (Lescrauwaet et al., 2022).

3. METHODOLOGY

This study applied a quantitative approach to assess how deepfake regulations impact content creation across social media, streaming platforms, and traditional media. Regulatory data

was collected from the World Bank's Governance Indicators and OECD's Regulatory Policy Outlook, by focusing on "Regulatory Quality" and "Rule of Law," it enabled cross-country comparisons among the United States, European Union, and China. Transparency reports from Facebook, Twitter, YouTube, and TikTok provided data on flagged and removed content, allowing a quantitative compliance analysis with deepfake regulations. Verification and public trust data were sourced from the Reuters Institute and EBU, while economic and public opinion data were gathered from the World Bank, ILO, and Statista.

To compare regulatory rigor, descriptive statistics and cross-country comparisons were calculated. Each region's regulatory quality score was standardized using:

$$Z = \frac{X - \mu}{\sigma}$$

where Z is the standardized score, XXX the observed regulatory quality, μ\muμ the mean, and σ\sigmaσ the standard deviation. Content moderation trends on social media and streaming platforms were analyzed via time-series and correlation analyses. The Pearson correlation coefficient, representing the relationship between flagged content volume and platform characteristics, was calculated as:

$$r = \frac{\sum(Xi - X^{-})(Yi - Y^{-})}{\sqrt{\sum(Xi - X^{-})^2 \sum(Yi - Y^{-})^2}}$$

where X and Y represent variables such as flagged content volume and user base size.
For traditional media, a chi-square test assessed the relationship between compliance practices (e.g., verification protocols, labeling) and public trust:

$$\chi^2 = \sum \frac{(O - E)^2}{E}$$

where O denotes observed frequencies and E expected frequencies. Additionally, a logistic regression model examined compliance practices' impact on public trust:

$$logit(p) = ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n$$

where p is the probability of public trust, β_0 the intercept, and β_1, $\beta_2 \ldots \beta_n$ are coefficients for predictors like labelling practices and verification standards.

To analyze social, ethical, and economic impacts, a multivariate regression was conducted with public trust, economic stability, and compliance costs as dependent variables. Independent variables included regulatory stringency, AI content prevalence, and public opinion scores, as shown in:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

where Y denotes a dependent variable (e.g., public trust), β_0 is the intercept, β_1, β_2, …, β_n are coefficients, and ϵ is the error term.

4. RESULTS

This analysis evaluates the regulatory approaches of the United States, the European Union, and China in relation to deepfake technology governance, focusing on the dimensions of Regulatory Quality and Rule of Law. The study aims to quantify and compare the regulatory rigor in each region to understand how these measures might influence the management of deepfake content across borders.

The quantitative assessment reveals distinct contrasts in regulatory effectiveness among the three regions. Table 1 summarises the mean and standard deviation scores for Regulatory Quality and Rule of Law, which were derived from World Bank and OECD datasets.

The U.S. demonstrates the highest levels of both Regulatory Quality (1.5) and Rule of Law (1.3), suggesting a robust framework potentially suited to effectively regulate emerging technologies like deepfakes. The EU shows similarly high, yet slightly lower scores, with Regulatory Quality at 1.2 and Rule of Law at 1.0. These values reflect a structured, transparency-focused approach that aligns with European Union directives on AI and digital governance. By contrast, China displays negative values (-0.5 for Regulatory Quality and -0.7 for Rule of Law), indicating a regulatory system focused more on state control than on transparency or individual autonomy.

The scatter plot (Fig. 1) further illustrates the relationship between Regulatory Quality and Rule of Law across these regions, emphasizing the clustering of the U.S. and EU at higher levels of governance quality compared to China. The line connecting the points highlights the strength of regulatory measures in both the U.S. and EU, where higher regulatory quality aligns closely

with robust rule enforcement. In contrast, China's positioning suggests less alignment between regulatory quality and rule of law, reflecting a regulatory model with distinct priorities.

In the grouped bar chart (Fig. 2), the stark differences in scores are visually reinforced, with the U.S. and EU outperforming China on both regulatory dimensions. The chart highlights how both regions have embraced a regulatory model aimed at supporting transparency and legal adherence, while China's model reflects a focus on social stability and control, potentially impacting its effectiveness in managing nuanced digital issues like deepfake content.

Table 1. Comparative summary of regulatory quality and rule of law by region

Indicator	U.S.	EU	China	Mean	Standard Deviation
Regulatory Quality	1.5	1.2	-0.5	0.733	1.079
Rule of Law	1.3	1.0	-0.7	0.533	1.079

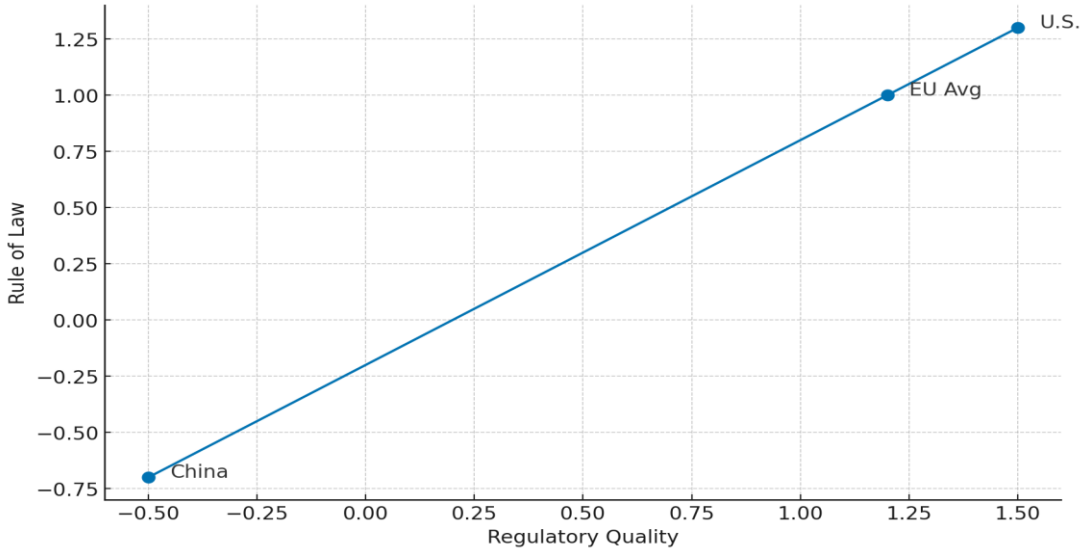

Fig. 1. Scatter plot of regulatory quality and rule of law

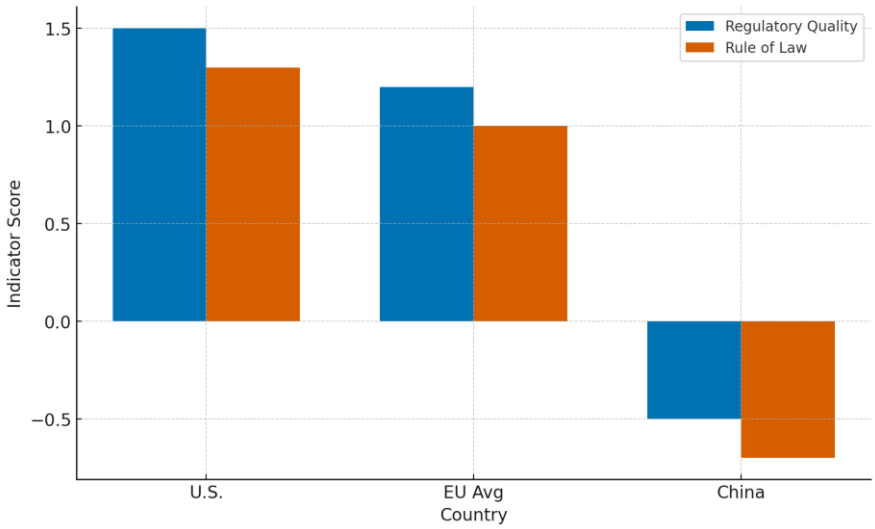

Fig. 2. Grouped bar chart of regulatory quality and rule of law by region

These findings emphasize the importance of a balanced regulatory approach that aligns both regulatory quality and rule of law to manage the risks and opportunities presented by deepfake technology. This contrast sets a foundation for further investigation into how these regulatory differences shape platform policies, compliance strategies, and public trust across each region.

4.1 Analyzing Social Media and Streaming Platform Regulations

This analysis assesses the effectiveness of major social media and streaming platforms such as Facebook, Twitter, YouTube, and TikTok, in moderating deepfake content by evaluating the responsiveness of flagged content being removed over time.

The results highlight distinct trends in content moderation effectiveness across platforms. Table 2 provides a summary of the total flagged and removed deepfake content volumes for each platform over a three-year period, along with the overall correlation result, which reflects the strength of the relationship between flagged and removed content.

The data in Table 2 reveal that YouTube and TikTok lead in flagged content, with YouTube removing 2,885 thousand instances and TikTok removing 3,107 thousand, indicating robust content moderation on these platforms. Twitter and Facebook follow closely, showing consistent detection and removal rates but at a slightly lower scale. The high overall correlation of 0.89 between flagged and removed content suggests that, across all platforms, increased detection aligns closely with higher removal rates, reflecting effective moderation practices industry-wide.

Table 2. Summary of total flagged and removed deepfake content by platform and overall correlation

Platform	Total Flagged Content (Thousands)	Total Removed Content (Thousands)	Correlation (Flagged vs Removed Content)
Facebook	2,509	2,305	0.89
Twitter	2,778	2,524	
YouTube	3,180	2,885	
TikTok	3,480	3,107	

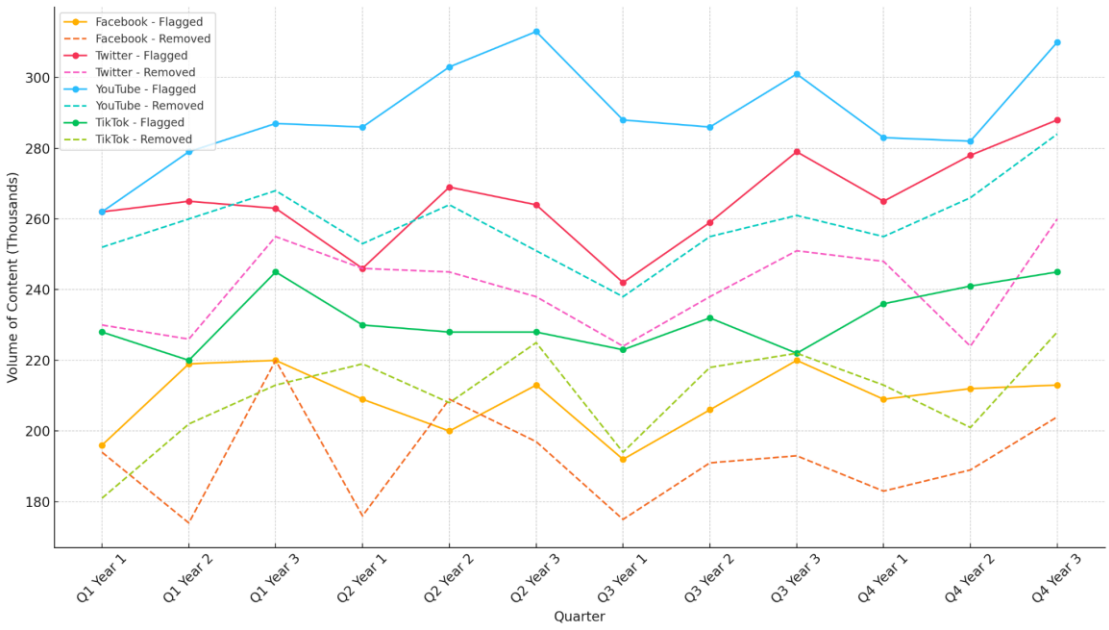

Fig. 3. Cumulative flagged and removed deepfake content across all platforms

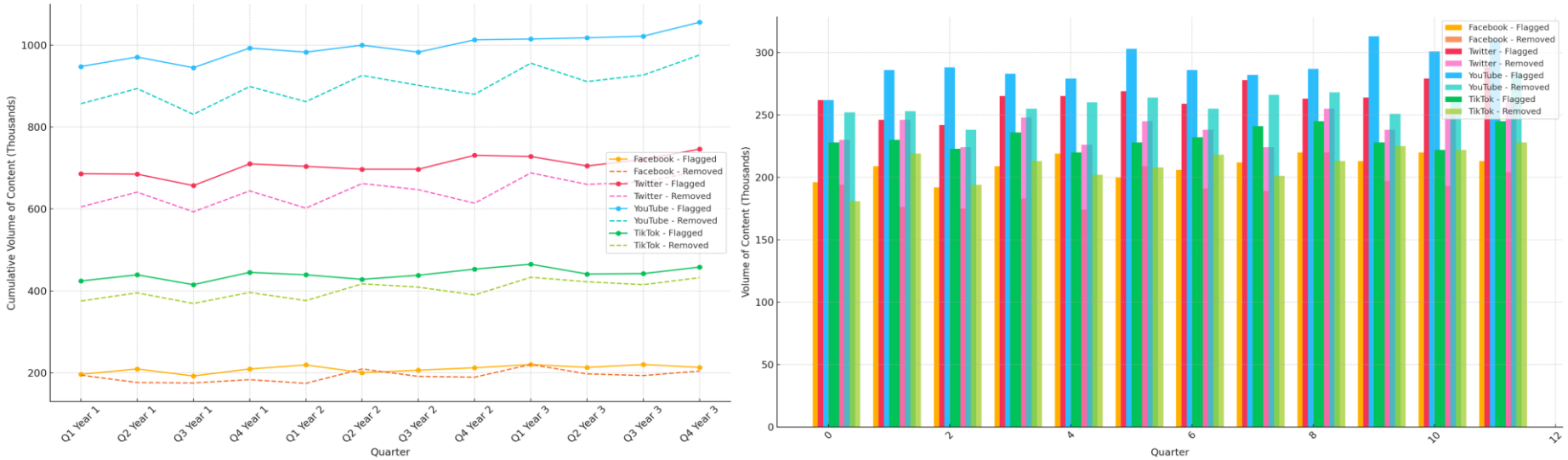

Fig. 4. Quarterly time series of flagged and removed deepfake content by platform

The stacked line chart in Fig. 3 shows the cumulative flagged and removed content across all platforms over time, demonstrating an overall upward trend in both flagged and removed content. This cumulative trend indicates that platforms are collectively enhancing their detection and removal efforts to address flagged deepfake content. The consistent rise in removal rates closely following flagged content aligns with increasing industry responsiveness to regulatory pressures, supporting an overall trend towards more active moderation.

Fig. 4 displays a quarterly time series and grouped bar chart comparing flagged and removed content across platforms, highlighting distinct moderation patterns. YouTube and TikTok exhibit high alignment between flagged and removed content, reflecting proactive real-time moderation. Conversely, Facebook and Twitter show moderate increases in flagged volumes with lower removal rates, suggesting varied thresholds for content removal. These differences underscore TikTok and YouTube's more active policies and support the study's goal of assessing regulatory effectiveness across platforms, offering insight into evolving content moderation practices.

4.2 Investigating Compliance in Traditional Media

This analysis examines the impact of compliance practices in traditional media on audience trust, focusing on the influence of verification protocols and labeling of synthetic media.

The results reveal a significant association between compliance practices and audience trust. Table 3 presents the outcome of the chi-square test, which demonstrates a statistically significant relationship between the presence of verification protocols and public trust in journalism, indicating that verification efforts play a critical role in fostering audience confidence.

The logistic regression analysis further underscores the role of verification protocols. As shown in Table 4, verification protocols have a significant positive coefficient (1.33, $p < 0.001$), suggesting that their presence substantially increases the likelihood of high trust in traditional media. Although labeling compliance also has a positive coefficient (0.48), it is not statistically significant, indicating that while labeling practices are beneficial, they are not as impactful as verification protocols in promoting public trust.

Table 3. Chi-square test result for association between compliance practices and audience trust

Test	p-value
Chi-Square Test	0.000053

The odds ratio bar chart in Fig. 5 provides a visual interpretation of the logistic regression results. The odds ratio for verification protocols is notably above 1, underscoring its strong association with increased trust. The confidence intervals indicate a statistically significant impact of verification, while the odds ratio for labeling compliance, though positive, shows a wider confidence interval, aligning with the lower significance level observed in the regression results.

The dot plot in Fig. 6 illustrates the predicted probabilities of high trust based on different combinations of compliance practices. The probability of high trust is highest when both verification and labeling compliance are present, indicating that these practices together bolster public trust in traditional media's handling of digital manipulation. The plot clearly shows that verification protocols alone result in a substantial increase in trust, reinforcing their critical role.

These findings highlight that compliance practices, particularly verification protocols, significantly enhance public trust in traditional media. These insights provide valuable direction for traditional media in reinforcing public trust through effective compliance measures.

4.3 Evaluating Social, Ethical, and Economic Implications

To evaluate deepfake regulations' social, ethical, and economic impacts on the entertainment industry, a regression analysis examined how compliance costs, AI content prevalence, and public opinion scores affect public trust and economic stability. The Public Trust Model (Table 5) reveals that compliance costs slightly reduce trust (coefficient = -0.10, p 0.001), possibly due to perceptions of resources being diverted from content quality. While AI content prevalence shows a positive but statistically insignificant association with trust (0.36), public opinion scores significantly boost trust (0.62, $p < 0.001$), underscoring the strong influence of favourable public sentiment on confidence in the sector.

Table 4. Logistic regression results for compliance practices influencing public trust

Variable	Coefficient	Standard error	z-value	p-value
Verification Protocol	1.326486	0.327300	4.052810	0.000051
Labeling Compliance	0.479829	0.323858	1.481606	0.138445

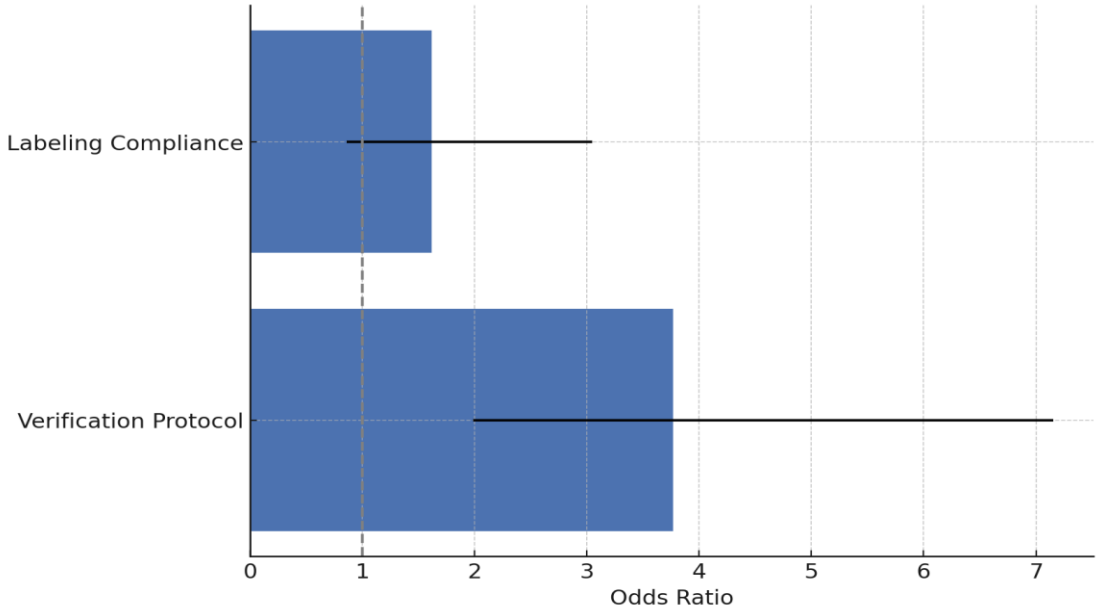

Fig. 5. Odds ratio of compliance practices on public trust

Fig. 6. Predicted probability of high trust by compliance practices (Dot plot)

Table 5. Regression results for factors influencing public trust

Variable	Coefficient	Standard Error	t-value	p-value
Compliance Costs	-0.10	0.03	-3.31	0.001
AI Content Prevalence	0.36	0.25	1.46	0.145
Public Opinion Scores	0.62	0.03	17.87	< 0.001

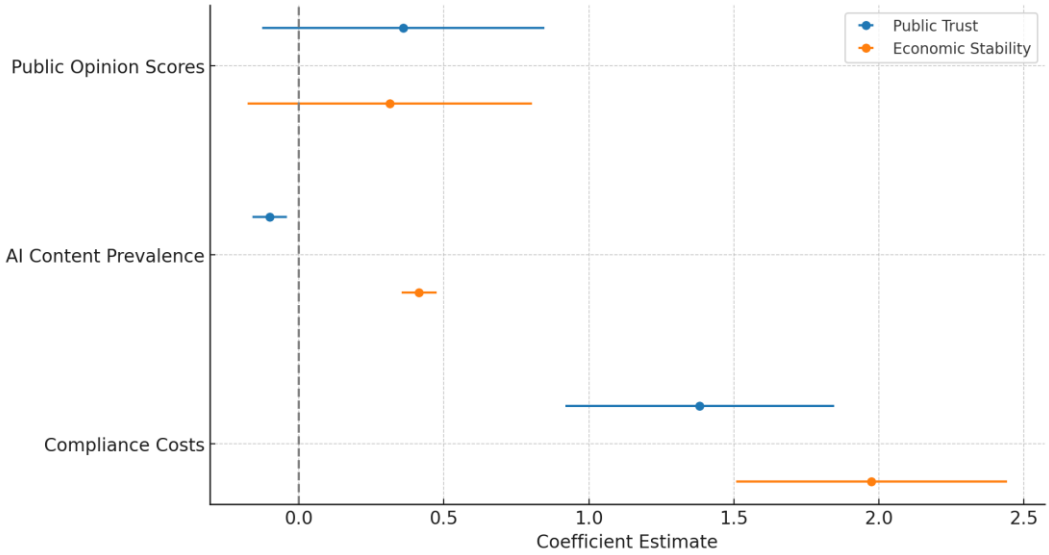

Fig. 7. Interaction plot of compliance costs and public opinion on predicted public trust

Table 6. Regression results for factors influencing economic stability

Variable	Coefficient	Standard Error	t-value	p-value
Compliance Costs	0.41	0.03	13.53	< 0.001
AI Content Prevalence	0.31	0.25	1.27	0.207
Public Opinion Scores	0.22	0.03	6.26	< 0.001

The interaction plot in Fig. 7 illustrates how compliance costs impact public trust at different public opinion levels. Public trust tends to decrease as compliance costs rise, but higher public opinion scores mitigate this effect, suggesting that positive public sentiment can offset the potential negative perception of high compliance costs.

In the Economic Stability Model (Table 6), compliance costs positively impact economic stability, with a coefficient of 0.41 ($p < 0.001$), indicating that investment in regulatory compliance aligns with greater financial resilience in the sector. AI content prevalence, although positive (0.31), does not significantly impact economic stability ($p = 0.207$), suggesting that while AI contributes to economic resilience, it is not a decisive factor. Public opinion scores enhance economic stability, with a significant coefficient of 0.22 ($p < 0.001$), underscoring the role of favorable public perceptions in promoting financial sustainability.

The coefficient plot in Fig. 8 provides a comparative view of the estimated effects for each variable across both models, highlighting the consistent positive influence of public opinion scores on both public trust and economic stability. Compliance costs show a mixed impact, being positive for economic stability but slightly negative for public trust.

The analysis reveals that compliance costs, AI content prevalence, and public opinion each play distinct roles in shaping public trust and economic stability in the entertainment sector. These findings indicate that the industry should prioritize maintaining positive public perceptions while balancing regulatory compliance investments to maximizYEEe both trust and economic stability.

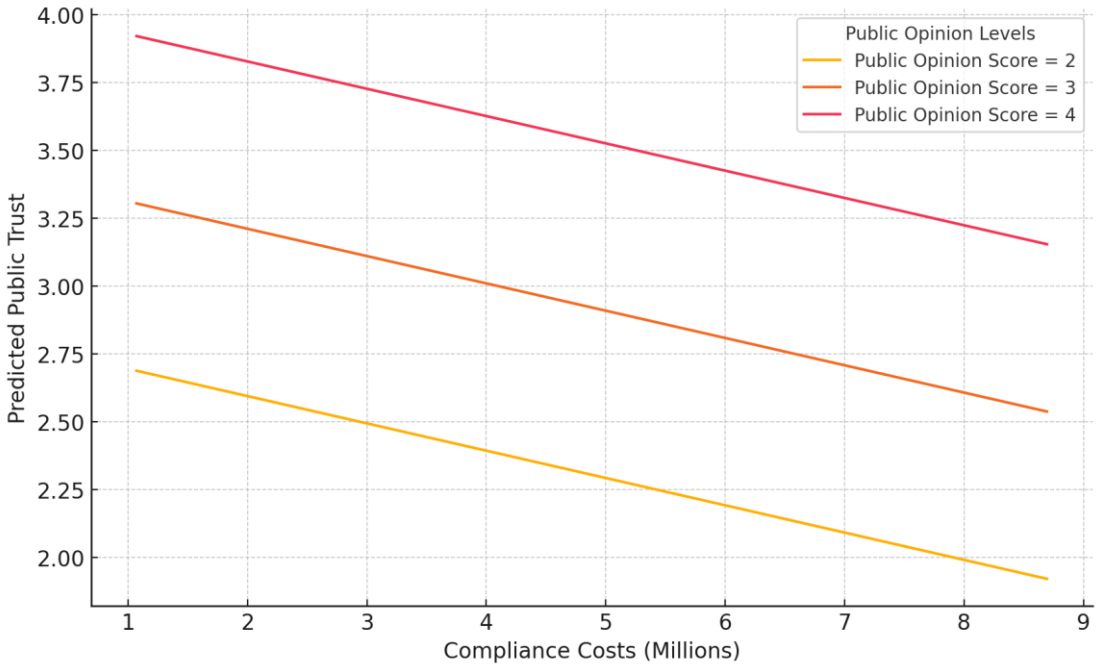

Fig. 8. Coefficient plot for public trust and economic stability models

5. DISCUSSION

The findings of this study emphasize the complexity of regulating deepfake technology in the entertainment sector, showcasing diverse approaches across the United States, the European Union, and China that reflect distinct cultural, political, and ethical imperatives. The United States' high levels of regulatory quality and rule of law (Table 1) suggest a strong institutional foundation that can effectively address emerging technological challenges, aligning with arguments by Montasari (2024) on the need for robust frameworks to manage deepfake risks. The EU's regulatory approach, while slightly less strict than that of the U.S., emphasizes transparency and individual rights, as highlighted in the Artificial Intelligence Act and Digital Services Act (European Parliament, 2023). This aligns with the EU's commitment to safeguarding personal privacy within digital governance frameworks, as argued by Krack et al. (2022). In contrast, China's lower regulatory quality and rule of law scores reflect a governance model focused on social stability and control, echoing Hemrajani's (2023) observations on China's emphasis on state-centered information management. These differences highlight the importance of tailoring deepfake regulations to regional priorities, where transparency and legal adherence in Western contexts contrast with China's prioritization of social order.

The analysis of social media and streaming platforms reveals significant advancements in moderating deepfake content, with a high overall correlation between flagged and removed content (Table 2), suggesting effective moderation efforts across major platforms. This high alignment is evident in YouTube and TikTok, which display robust removal rates in response to flagged content, demonstrating responsive policies in line with increased regulatory pressures (Fig. 4). However, platforms like Facebook and Twitter exhibit lower removal rates relative to flagged content, indicating that varying content moderation standards may influence their efficacy. These results parallel findings by Malik, Surbhi, and Roy (2024), who noted the distinct policies employed by each platform in managing harmful content. The results further suggest that platforms with stricter detection and removal policies, such as YouTube and TikTok, achieve greater alignment with regulatory expectations, supporting the argument by Park and Rohatgi (2024) on the importance of adaptable frameworks in moderating AI-generated media. Thus, as platforms enhance their moderation practices, they contribute to a more responsible digital ecosystem that balances free expression with harm prevention, addressing

ethical concerns raised by Baik and Sridharan (2023) on censorship and diverse expression.

In the context of traditional media, compliance practices appear to have a marked impact on public trust. The chi-square test and logistic regression results reveal that verification protocols significantly enhance audience confidence in journalistic content, aligning with Spyropoulos et al. (2023), who argue that transparency and verification protocols reinforce public trust in journalism. The significant odds ratio for verification protocols (Table 4) highlights the weight that audiences place on verified information in an era of digital manipulation. Labeling compliance, while beneficial, showed a lesser impact, suggesting that while audiences value disclosure practices, the presence of strict verification standards is more central to trust-building, as suggested by Sharma and Rout (2024). Fig. 6 further illustrates this trend, with predicted probabilities of high trust rising most notably when both verification and labeling compliance are present. These findings reinforce Garon's (2023) stance on the necessity of labeling for informed media consumption, though verification protocols evidently carry greater influence over public perception.

Evaluating the social, ethical, and economic implications of deepfake regulations reveals nuanced interactions between compliance costs, AI content prevalence, and public opinion. Compliance costs, which negatively impact public trust but bolster economic stability (Table 5), suggest a perceived trade-off where audiences may view high regulatory expenditures as diverting resources from creative quality (Davis, 2024). The interaction plot (Fig. 7) elucidates how positive public opinion mitigates the adverse effect of compliance costs on trust, underscoring the importance of favourable public sentiment for maintaining confidence in regulated media environments. To mitigate these biases, multiple strategies were employed. Data sources were cross-verified to ensure reliability, comparing transparency reports from platforms like YouTube, Facebook, and TikTok against independent audits. Standardized measures, such as the World Bank's Governance Indicators and OECD's Regulatory Policy Outlook, ensured uniformity in evaluating regulatory quality and rule of law across regions. Robust statistical techniques were applied to minimize the impact of outliers, and sensitivity tests were conducted to assess the stability of findings, further ensuring the rigor and reliability of the analysis. Public opinion's positive influence on both public trust and economic stability, as reflected in the regression results, underscores the centrality of audience perception, corroborating findings by Farouk and Fahmi (2024) on the trust-enhancing role of public sentiment. AI content prevalence, while positively associated with both outcomes, showed a lesser influence, aligning with Gao et al. (2023) who suggest that while audiences appreciate AI-enhanced media, trust is more deeply influenced by ethical considerations and transparency. In this context, compliance practices that engage positively with public sentiment while ensuring regulatory adherence may best support a sustainable entertainment sector.

6. CONCLUSION AND RECOMMENDATION

This study reveals the necessity of region-specific regulatory approaches for managing deepfake technology within the entertainment sector, highlighting cultural, ethical, and economic factors that inform policies in the United States, European Union, and China. The U.S. and EU show high alignment between regulatory quality and rule of law, favouring transparency and individual rights, while China emphasises state control for social stability. Social media and streaming platforms vary in their effectiveness, with platforms like YouTube and TikTok showing strong alignment with regulatory expectations. In traditional media, verification protocols significantly enhance public trust, underscoring the importance of transparency. Compliance costs and public opinion critically influence industry trust and stability, demonstrating that well-designed regulations can foster both trust and economic resilience. Therefore, the following are recommended:

1. Strengthen international regulatory alignment to ensure consistency in transparency, labeling, and compliance, addressing the global impact of deepfake content and enhancing cross-border trust.
2. Emphasize verification protocols in media as a priority over labeling, reinforcing public trust by ensuring high standards of authenticity and reliability in traditional journalism.
3. Enhance AI-driven detection on social media platforms for more effective real-time moderation of deepfake content, supporting proactive compliance with regulatory standards.

4. Expand public digital literacy initiatives to empower audiences in recognizing manipulated media, thus promoting a more informed, resilient public in an AI-enhanced media environment.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

Abdallah, M., & Salah, M. (2023). Artificial intelligence and intellectual properties: Legal and ethical considerations. *International Journal of Intelligent Systems and Applications in Engineering, 12*(1), 368–376. https://www.researchgate.net/publication/376885311_Artificial_Intelligence_and_Intellectual_Properties_Legal_and_Ethical_Considerations

ACLU. (2022). ACLU v. Clearview AI. *American Civil Liberties Union*. https://www.aclu.org/cases/aclu-v-clearview-ai

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the future: The interplay of artificial intelligence, innovation, and competitiveness and its effect on the global economy. *Asian Journal of Economics, Business and Accounting, 24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Akinola, O. I., Olaniyi, O. O., Ogungbemi, O. S., Oladoyinbo, O. B., & Olisa, A. O. (2024). Resilience and recovery mechanisms for software-defined networking (SDN) and cloud networks. *Journal of Engineering Research and Reports, 26*(8), 112–134. https://doi.org/10.9734/jerr/2024/v26i81234

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The interconnectedness of earnings management, corporate governance failures, and global economic stability: A critical examination of the impact of earnings manipulation on financial crises and investor trust in global markets. *Asian Journal of Economics, Business and Accounting, 24*(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542

Alcántara, J. C., Tasic, I., & Cano, M.-D. (2024). Enhancing digital identity: Evaluating avatar creation tools and privacy challenges for the metaverse. *Information, 15*(10), 624. https://doi.org/10.3390/info15100624

Al-kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., & Alfandi, O. (2024a). A systematic review and analysis of ethical challenges of generative AI: An interdisciplinary perspective. *SSRN*. https://doi.org/10.2139/ssrn.4833030

Al-kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., & Alfandi, O. (2024b). Ethical challenges and solutions of generative AI: An interdisciplinary perspective. *Informatics, 11*(3), 58. https://doi.org/10.3390/informatics11030058

Allan, J., Belz, S., Hoeveler, A., Hugas, M., Okuda, H., Patri, A., Rauscher, H., Silva, P., Slikker, W., Sokull-Kluettgen, B., Tong, W., & Anklam, E. (2021). Regulatory landscape of nanotechnology and nanoplastics from a global perspective. *Regulatory Toxicology and Pharmacology, 122*, 104885. https://doi.org/10.1016/j.yrtph.2021.104885

Allyn, B. (2024, September 29). California Gov. Newsom vetoes AI safety bill that divided Silicon Valley. *NPR*. https://www.npr.org/2024/09/20/nx-s1-5119792/newsom-ai-bill-california-sb1047-tech

Arigbabu, A. S., Olaniyi, O. O., & Adeola, A. (2024). Exploring primary school pupils' career aspirations in Ibadan, Nigeria: A qualitative approach. *Journal of Education, Society and Behavioural Science, 37*(3), 1–16. https://doi.org/10.9734/jesbs/2024/v37i31308

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data governance in AI-enabled healthcare systems: A case of the Project Nightingale. *Asian Journal of Research in Computer Science, 17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., & Olaniyi, O. O. (2024). Evaluating the trade-offs between wireless security and performance in IoT networks: A case study of web applications in AI-driven home appliances. *Journal of Engineering Research and Reports, 26*(8), 411–432. https://doi.org/10.9734/jerr/2024/v26i81255

Baik, J., & Sridharan, H. (2023). Civil rights audits as counterpublic strategy: Articulating the responsibility and failure to care for marginalized communities in platform governance. *Information, Communication & Society, 27*(5), 1–20. https://doi.org/10.1080/1369118x.2023.2227685

Birrer, A., & Just, N. (2024). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. *New Media & Society*. https://doi.org/10.1177/14614448241253138

Braine, N. (2020). Autonomous health movements: Criminalization, de-medicalization, and community-based direct action. *Health and Human Rights, 22*(2), 85–97. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7762925/

Business Matters. (2024). "Deepfake" music start-up Voicify faces copyright dispute. *Business Matters*. https://bmmagazine.co.uk/news/deepfake-music-start-up-voicify-faces-copyright-dispute/

Chapdelaine, P., & McLeod Rogers, J. (2021). Contested sovereignties: States, media platforms, peoples, and the regulation of media content and big data in the networked society. *Laws, 10*(3), 66. https://doi.org/10.3390/laws10030066

Chawki, M. (2024). Navigating legal challenges of deepfakes in the American context: A call to action. *Cogent Engineering, 11*(1). https://doi.org/10.1080/23311916.2024.2320971

Cheong, I., Caliskan, A., & Kohno, T. (2024). Safeguarding human values: Rethinking US law for generative AI's societal impacts. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00451-4

Cooke, C. (2024). BPI threatens to sue voice cloning site Voicify. *CMU | the Music Business Explained*. https://completemusicupdate.com/bpi-threatens-to-sue-voice-cloning-site-voicify/

Dame Adjin-Tettey, T. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent Arts & Humanities, 9*(1). https://doi.org/10.1080/23311983.2022.2037229

Davis, J. L. (2024). The failure-speed ethos: Notes from a glocal startup scene. *Information, Communication & Society*, 1–18. https://doi.org/10.1080/1369118x.2024.2343807

Delfino, R. (2024). Pay-to-play: Access to justice in the era of AI and deepfakes. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4722364

de-Lima-Santos, M.-F., Yeung, W. N., & Dodds, T. (2024). Guiding the way: A comprehensive examination of AI guidelines in global media. *AI & Society*. https://doi.org/10.1007/s00146-024-01973-5

Deng, Z., & Chen, Z. (2023). Balancing creative expression and societal well-being: A comprehensive regulatory framework for the Chinese video game industry. *Journal of the Knowledge Economy*. https://doi.org/10.1007/s13132-023-01491-7

Department of Homeland Security. (2023). Increasing threat of deepfake identities. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

DiGiacomo, D. K., Hodgin, E., Kahne, J., Alkam, S., & Taylor, C. (2023). Assessing the state of media literacy policy in U.S. K-12 schools. *Journal of Children and Media, 17*(3), 336–352. https://doi.org/10.1080/17482798.2023.2201890

Eurojust. (2022). Digital Services Act: Ensuring a safe and accountable online environment. *Eurojust | European Union Agency for Criminal Justice Cooperation*. https://www.eurojust.europa.eu/publication/digital-services-act-ensuring-safe-and-accountable-online-environment

European Commission. (2021). Data protection in the EU. *Commission.europa.eu*. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

European Parliament. (2023). EU AI Act: First regulation on artificial intelligence. *European Parliament*.

https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Evans, B. (2023). The problem of deepfake pornography. *Harvard Undergraduate Law Review*. https://hulr.org/law-in-the-news/4pl86959avgiap782c5pvb2a4tnz30

Farouk, M. A., & Fahmi, B. M. (2024). Deepfakes and media integrity: Navigating the new reality of synthetic content. *Journal of Media and Interdisciplinary Studies, 3*(9). https://doi.org/10.21608/jmis.2024.275298.1027

Florea, M., & Esteves, B. (2023). Is automated consent in solid GDPR-compliant? An approach for obtaining valid consent with the Solid protocol. *Information, 14*(12), 631. https://doi.org/10.3390/info14120631

Gao, B., Wang, Y., Xie, H., & Hu, Y. (2023). Artificial intelligence in advertising: Advancements, challenges, and ethical considerations in targeting, personalization, content creation, and ad optimization. *SAGE Open, 13*(4). https://doi.org/10.1177/21582440231210759

Garon, J. (2023). A practical introduction to generative AI, synthetic media, and the messages found in the latest medium. *Papers.ssrn.com*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4388437

Gavrilova, N., Gershman, M., & Thurner, T. W. (2022). Policy challenges and recommendations in support of Moscow's creative industries – Viewpoints of practitioners. *Creative Industries Journal, 16*(2), 1–16. https://doi.org/10.1080/17510694.2022.2062946

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., & Olaniyi, O. O. (2024). Augmenting data privacy protocols and enacting regulatory frameworks for cryptocurrencies via advanced blockchain methodologies and artificial intelligence. *Journal of Engineering Research and Reports, 26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

George, D. A. S., & George, A. S. H. (2023). Deepfakes: The evolution of hyper-realistic media manipulation. *Partners Universal Innovative Research Publication, 1*(2), 58–74. https://doi.org/10.5281/zenodo.10148558

Gregory, S. (2021). Deepfakes, misinformation and disinformation, and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism. *Journalism, 23*(3), 146488492110606. https://doi.org/10.1177/14648849211060644

Haggart, B., & Keller, C. I. (2021). Democratic legitimacy in global platform governance. *Telecommunications Policy, 45*(6), 102152. https://doi.org/10.1016/j.telpol.2021.102152

Hemrajani, A. (2023). China's new legislation on deepfakes: Should the rest of Asia follow suit? *Thediplomat.com*. https://thediplomat.com/2023/03/chinas-new-legislation-on-deepfakes-should-the-rest-of-asia-follow-suit/

Hoofnagle, C. J., Sloot, B. V. D., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Huang, K., Joshi, A., Dun, S., & Hamilton, N. (2024). AI regulations. *Future of Business and Finance*, 61–98. https://doi.org/10.1007/978-3-031-54252-7_3

Jenny, F. (2021). Competition law enforcement and regulation for digital platforms and ecosystems: Understanding the issues, facing the challenges and moving forward. *Papers.ssrn.com*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3857507

Jin, T., & Shao, Y. (2024). Exploring community resilience based on co-produced micro-regeneration projects in China: Two case studies. *Journal of Urban Affairs*, 1–18. https://doi.org/10.1080/07352166.2024.2360485

Joeaneke, P. C., Kolade, T. M., Val, O. O., Olisa, A. O., Joseph, S. A., & Olaniyi, O. O. (2024). Enhancing security and traceability in aerospace supply chains through blockchain technology. *Journal of Engineering Research and Reports, 26*(10), 114–135. https://doi.org/10.9734/jerr/2024/v26i101294

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting autonomous UAVs

from GPS spoofing and jamming: A comparative analysis of detection and mitigation techniques. *Journal of Engineering Research and Reports, 26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., & Nwokonkwo, O. C. (2024). Advancing COVID-19 prediction with deep learning models: A review. 2024 *International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, Omu-Aran, Nigeria, 2024, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Joseph, S. A. (2024). Balancing data privacy and compliance in blockchain-based financial systems. *Journal of Engineering Research and Reports, 26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

Knott, A., Pedreschi, D., Jitsuzumi, T., Leavy, S., Eyers, D., Chakraborti, T., Trotman, A., Sundareswaran, S., Baeza-Yates, R., Biecek, P., Weller, A., Teal, P. D., Basu, S., Haklidir, M., Morini, V., Russell, S., & Bengio, Y. (2024). AI content detection in the emerging information ecosystem: New obligations for media and tech companies. *Ethics and Information Technology, 26*(4). https://doi.org/10.1007/s10676-024-09795-1

Kothari, A., & Cruikshank, S. A. (2021). Artificial intelligence and journalism: An agenda for journalism research in Africa. *African Journalism Studies, 43*(1), 1–17. https://doi.org/10.1080/23743670.2021.1999840

Krack, N., Beudels, M., Valcke, P., & Kuczerawy, A. (2022). AI in the Belgian media landscape: When fundamental risks meet regulatory complexities. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4498265

Lescrauwaet, L., Wagner, H., Yoon, C. Y., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation. *Law and Economics, 16*(3), 202–220. https://doi.org/10.35335/laweco.v16i3.61

Luo, M., Hancock, J. T., & Markowitz, D. M. (2020). Credibility perceptions and detection accuracy of fake news headlines on social media: Effects of truth-bias and endorsement cues. *Communication Research, 49*(2), 009365022092132. https://doi.org/10.1177/0093650220921321

Maddaus, G. (2024). Entertainment industry backs bill to outlaw AI deepfakes. *Variety*. https://variety.com/2024/politics/news/ai-bill-outlaw-no-fakes-sag-aftra-1236091652/

Malik, S., Surbhi, A., & Roy, D. (2024). Blurring boundaries between truth and illusion: Analysis of human rights and regulatory concerns arising from abuse of deepfake technology. *AIP Conference Proceedings, 3220*(1), 050016. https://doi.org/10.1063/5.0234995

Mania, K. (2022). Legal protection of revenge and deepfake porn victims in the European Union: Findings from a comparative legal study. *Trauma, Violence, & Abuse, 25*(1), 152483802211437. https://doi.org/10.1177/15248380221143772

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly, 38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

Metwally, A. (2019). Manipulated media: Examining California's deepfake bill. *Harvard Journal of Law & Technology*. https://jolt.law.harvard.edu/digest/manipulated-media-examining-californias-deepfake-bill

Montasari, R. (2024). Responding to deepfake challenges in the United Kingdom: Legal and technical insights with recommendations. *Advanced Sciences and Technologies for Security Applications*, 241–258. https://doi.org/10.1007/978-3-031-50454-9_12

Moreno, F. R. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. *International Review of Law Computers & Technology, 38*(3), 1–30. https://doi.org/10.1080/13600869.2024.2324540

Murray, M. D. (2024). Generative artifice: Regulation of deepfake exploitation and deception under the First Amendment. *SSRN*. https://doi.org/10.2139/ssrn.4872032

Nanni, R., Bizzaro, P. G., & Napolitano, M. (2024). The false promise of individual digital sovereignty in Europe: Comparing artificial intelligence and data regulations in China and the European Union. *Policy & Internet*. https://doi.org/10.1002/poi3.424

Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: An in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing, 6*(5), 1–12. https://research.tensorgate.org/index.php/IJIAC/article/view/61

Noti-Victor, J. (2024). Regulating hidden AI authorship. *SSRN*. https://doi.org/10.2139/ssrn.4909907

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming remote workforce cyber threats: A comprehensive ransomware and bot net defense strategy utilizing VPN networks. *Journal of Engineering Research and Reports, 26*(8), 161–184. https://doi.org/10.9734/jerr/2024/v26i81237

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating privacy by design principles in the modification of AI systems in preventing breaches across multiple environments, including public cloud, private cloud, and on-prem. *Journal of Engineering Research and Reports, 26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science, 17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics. *Asian Journal of Advanced Research and Reports, 18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Olaniyi, O. O. (2024). Ballots and padlocks: Building digital trust and security in democracy through information governance strategies and blockchain technologies. *Asian Journal of Research in Computer Science, 17*(5), 172–189. https://doi.org/10.9734/ajrcos/2024/v17i5447

Olaniyi, O. O., Ezeugwa, F. A., Okatta, C. G., Arigbabu, A. S., & Joeaneke, P. C. (2024). Dynamics of the digital workforce: Assessing the interplay and impact of AI, automation, and employment policies. *Archives of Current Research International, 24*(5), 124–139. https://doi.org/10.9734/acri/2024/v24i5690

Olaniyi, O. O., Olaoye, O. O., & Okunleye, O. J. (2023). Effects of information governance (IG) on profitability in the Nigerian banking sector. *Asian Journal of Economics, Business and Accounting, 23*(18), 22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. *Journal of Engineering Research and Reports, 26*(6), 32. https://doi.org/10.9734/JERR/2024/v26i61160

Olaniyi, O. O., Ugonnia, J. C., Olaniyi, F. G., Arigbabu, A. T., & Adigwe, C. S. (2024). Digital collaborative tools, strategic communication, and social capital: Unveiling the impact of digital transformation on organizational dynamics. *Asian Journal of Research in Computer Science, 17*(5), 140–156. https://doi.org/10.9734/ajrcos/2024/v17i5444

Olateju, O. O., Okon, S. U., Igwenagu, U. T. I., Salami, A. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). Combating the challenges of false positives in AI-driven anomaly detection systems and enhancing data security in the cloud. *Asian Journal of Research in Computer Science, 17*(6), 264–292. https://doi.org/10.9734/ajrcos/2024/v17i6472

Olateju, O. O., Okon, S. U., Olaniyi, O. O., Samuel-Okon, A. D., & Asonze, C. U. (2024). Exploring the concept of explainable AI and developing information governance standards for enhancing trust and transparency in handling customer data. *Journal of Engineering Research and Reports, 26*(7), 244–268. https://doi.org/10.9734/jerr/2024/v26i71206

Park, T. J., & Rohatgi, A. (2024). Balancing the platform responsibility paradox: A case for

amplification regulation to mitigate the spread of harmful but legal content online. *Computer Law & Security Review, 52*, 105960. https://doi.org/10.1016/j.clsr.2024.105960

Pickering, B. (2021). Trust, but verify: Informed consent, AI technologies, and public health emergencies. *Future Internet, 13*(5), 132. https://doi.org/10.3390/fi13050132

Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and edge computing-based computer forensics: Challenges and open problems. *Electronics, 10*(11), 1229. https://doi.org/10.3390/electronics10111229

Ramirez, D., & Andrada, C. (2024). 70 deepfake statistics you need to know (2024). *Spiralytics; Spiralytics Inc.* https://www.spiralytics.com/blog/deepfake-statistics/

Salami, A. A., Igwenagu, U. T. I., Mesode, C. E., Olaniyi, O. O., & Oladoyinbo, O. B. (2024). Beyond conventional threat defense: Implementing advanced threat modeling techniques, risk modeling frameworks and contingency planning in the healthcare sector for enhanced data security. *Journal of Engineering Research and Reports, 26*(5), 304–323. https://doi.org/10.9734/jerr/2024/v26i51156

Samuel-Okon, A. D., Akinola, O. I., Olaniyi, O. O., Olateju, O. O., & Ajayi, S. A. (2024). Assessing the effectiveness of network security tools in mitigating the impact of deepfakes AI on public trust in media. *Archives of Current Research International, 24*(6), 355–375. https://doi.org/10.9734/acri/2024/v24i6794

Samuel-Okon, A. D., Olateju, O. O., Okon, S. U., Olaniyi, O. O., & Igwenagu, U. T. I. (2024). Formulating global policies and strategies for combating criminal use and abuse of artificial intelligence. *Archives of Current Research International, 24*(5), 612–629. https://doi.org/10.9734/acri/2024/v24i5735

Selesi-Aina, O., Obot, N. E., Olisa, A. O., Gbadebo, M. O., Olateju, O. O., & Olaniyi, O. O. (2024). The future of work: A human-centric approach to AI, robotics, and cloud computing. *Journal of Engineering Research and Reports, 26*(11), 62–87. https://doi.org/10.9734/jerr/2024/v26i111315

Shao, Z., Zhao, R., Yuan, S., Ding, M., & Wang, Y. (2022). Tracing the evolution of AI in the past decade and forecasting the emerging trends. *Expert Systems with Applications, 209*, 118221. https://doi.org/10.1016/j.eswa.2022.118221

Sharma, R., & Rout, A. (2024). Through the digital maze: Media regulation for ethical journalism in a disinformation age. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4799566

Sobel, B. (2024). A real account of deep fakes. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4829598

Spyropoulos, A. Z., Bratsas, C., Makris, G. C., Garoufallou, E., & Tsiantos, V. (2023). Interoperability-enhanced knowledge management in law enforcement: An integrated data-driven forensic ontological approach to crime scene analysis. *Information, 14*(11), 607. https://doi.org/10.3390/info14110607

Tan, C. (2022). Regulating disinformation on Twitter and Facebook. *Griffith Law Review, 31*(4), 1–24. https://doi.org/10.1080/10383441.2022.2138140

Thomas, S. (2024). AI and actors: Ethical challenges, cultural narratives, and industry pathways in synthetic media performance. *Emerging Media*. https://doi.org/10.1177/27523543241289108

Thomson, T. J., Angus, D., Dootson, P., Hurcombe, E., & Smith, A. (2020). Visual mis/disinformation in journalism and public communications: Current verification practices, challenges, and future opportunities. *Journalism Practice, 16*(5), 938–962. https://doi.org/10.1080/17512786.2020.1832139

Thongmeensuk, S. (2024). Rethinking copyright exceptions in the era of generative AI: Balancing innovation and intellectual property protection. *The Journal of World Intellectual Property, 27*(2). https://doi.org/10.1111/jwip.12301

TikTok. (2019). Partnering with our industry to advance AI transparency and literacy. *Newsroom | TikTok*. https://newsroom.tiktok.com/en-us/partnering-with-our-industry-to-advance-ai-transparency-and-literacy

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1). https://doi.org/10.1177/2056305120903408

Wakefield, J. (2021). Google, Facebook, Twitter grilled in US on fake news. *BBC News*. https://www.bbc.com/news/technology-56523378

Weikmann, T., Greber, H., & Nikolaou, A. (2024). After deception: How falling for a deepfake affects the way we see, hear, and experience media. *The International Journal of Press/Politics*. https://doi.org/10.1177/19401612241233539

Wolniak, R., & Stecuła, K. (2024). Artificial intelligence in smart cities—Applications, barriers, and future directions: A review. *Smart Cities, 7*(3), 1346–1389. https://doi.org/10.3390/smartcities7030057

Yang, X., Chai, L., Bist, R. B., Subedi, S., & Wu, Z. (2022). A deep learning model for detecting cage-free hens on the litter floor. *Animals, 12*(15), 1983. https://doi.org/10.3390/ani12151983

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/127855