



INTERNATIONAL JOURNAL
OF LAW, GOVERNMENT
AND COMMUNICATION
(IJLGC)

www.gaexcellence.com/ijlgc



MALAYSIA'S POLICY READINESS FOR SYNTHETIC MEDIA AND DEEPPAKES REGULATION

Aufa Muqree¹, Noor Aziah Abdullah^{2*}

¹School of Multimedia Technology and Communication, Universiti Utara Malaysia, Malaysia

 m_aufa_muqree@smmtc.uum.edu.my

 <https://orcid.org/0009-0002-7507-5464>

²School of Multimedia Technology and Communication, Universiti Utara Malaysia, Malaysia

 nooraziah@uum.edu.my

 <https://orcid.org/0000-0002-0557-2409>

*Corresponding Author

Article Info:

Article history:

Received date: 06.07.2026

Revised date: 28.07.2026

Accepted date: 30.08.2026

Published date: 21.09.2026

To cite this document:

Nazree, M. A. M. & Abdullah N. A. Malaysia's Policy Readiness For Synthetic Media And Deepfakes Regulation. *International Journal of Law, Government and Communication*, 11(45), 547-562.

Abstract:

The rapid advancement of artificial intelligence (AI) has transformed the creation and circulation of digital media, including synthetic media and deepfakes capable of realistically imitating individuals. Although Malaysian scholarship and policy discussions have addressed digital misinformation, online harms, and AI governance, limited empirical research has examined the adequacy of existing legal instruments specifically for synthetic media and deepfake-related harms. Drawing on the regulative pillar of Institutional Theory, this study examines the extent to which Malaysia's formal laws, regulatory mechanisms, and enforcement arrangements are prepared to address such harms. A qualitative exploratory design was used. Four purposively selected participants representing government communication, public relations, media law, and media industry practice were interviewed to provide cross-sector perspectives. Document analysis of relevant Malaysian legislation, regulatory policies, official guidance, and government materials was used to triangulate and contextualise the interview findings. Thematic analysis identified four main themes: fragmented legal coverage, definitional uncertainty, reactive enforcement, and the need for stronger platform accountability and AI-specific legal safeguards. Existing instruments, including the Communications and Multimedia Act 1998, Defamation Act 1957, Evidence Act 1950, Penal Code, and Online Safety Act 2025, may address particular consequences of deepfake misuse, but they do not constitute a law specifically designed for synthetic media. The study therefore finds that Malaysia demonstrates partial regulative readiness. Greater readiness requires clearer definitions of synthetic media and deepfakes, proportionate disclosure and liability rules, faster enforcement and takedown procedures, improved digital-evidence processes, and clearer platform responsibilities.

DOI: 10.35631/IJLGC.1145035 **Keyword:**

Deepfake, Institutional Theory, Media Governance In Malaysia,
Policy Readiness, Synthetic Media



© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact ijlge@gaexcellence.com.

Introduction

The rapid development of artificial intelligence (AI) has reshaped the way digital media content is produced, edited, distributed and consumed. One significant outcome is the emergence of synthetic media and deep-fake technologies. In studies by Chesney and Citron (2019), synthetic media is defined as digital content such as images, videos, audio or text that is generated or manipulated using AI technologies. Deepfakes on the other hand is a subset of synthetic media, use deep-learning techniques to imitate a person's face, voice, or actions in a highly realistic manner (Mirsky & Lee, 2021).

Although synthetic media can be used positively in entertainment, education, advertising, film production, and digital communication, its misuse has raised serious legal and regulatory concerns. Deepfake technologies can be used to produce misleading videos, impersonate individuals, manipulate political communication, create fraudulent content, and damage personal reputations. These risks are worsened by the increasing accessibility of AI tools, where users with limited technical knowledge can generate realistic, manipulated content through mobile applications, online platforms, and open-source software (Kietzmann et al., 2020; Westerlund, 2019).

Globally, the rise of synthetic media has encouraged governments and regulatory bodies to develop legal responses that can manage the risks of AI-generated content. The European Union approved a risk-based strategy known as the Artificial Intelligence Act which includes transparency requirements for specific AI-generated or altered information (European Parliament & Council of the European Union, 2024). Other jurisdictions have also considered legal measures involving mandatory labelling, platform responsibility, disclosure requirements, and criminal liability for harmful deepfake misuse (Calo, 2017; Chesney & Citron, 2019). These developments show that legal readiness is increasingly important in addressing the challenges created by synthetic media.

In Malaysia, deepfake regulation remains an emerging issue. Existing laws such as the Communications and Multimedia Act 1998, Defamation Act 1957, Evidence Act 1950 and Penal Code may be relevant to particular harms caused by synthetic media, but these instruments were not designed specifically for modern generative AI. The National Guidelines on AI Governance and Ethics, the Communications and Multimedia (Amendment) Act 2025, and the Online Safety Act 2025 are examples of recent developments that show ongoing efforts to improve digital governance and responsible AI use (Ministry of Science, Technology and

Innovation, 2024). Nevertheless, a research gap remains. Existing Malaysian legal and policy discussions address online harms and AI governance but limited empirical research has examined how adequate the existing legal framework is specifically for synthetic media and deepfake-related harms (Sahak et al., 2025). This leaves uncertainty in areas such as consent, identity misuse, digital evidence, platform responsibility, and liability for AI-generated content. Drawing on the regulative pillar of Institutional Theory, this study therefore examines the extent to which Malaysia's formal laws, regulatory mechanisms, and enforcement arrangements are prepared to address harms associated with synthetic media and deepfake technologies.

Literature Review

Synthetic Media and Deepfake

Synthetic media refers to digital content that is created or altered using artificial intelligence technologies which includes AI-generated images, avatars, videos, audio recording and written content (Farid, 2022). According to Farid (2022), deepfakes are a specific form of synthetic media that uses machine-learning models to generate or manipulate realistic representations of real individuals. These technologies are commonly associated with Generative Adversarial Networks (GANs), where one model generates synthetic content while another model evaluates its realism (Goodfellow et al., 2014; Mirsky & Lee, 2021).

The realism of deepfake content has improved significantly due to advances in deep learning, image synthesis, voice cloning, and facial reenactment technologies (Tolosana et al., 2020). As a result, manipulated content may appear authentic to ordinary viewers and may even be difficult to detect without technical tools. This creates serious challenges for legal institutions, media organisations, regulators, and the public because it becomes increasingly difficult to distinguish between authentic and manipulated media (Verdoliva, 2020).

The growth of deepfake technologies has also been accelerated by the availability of opensource software, mobile applications, and online AI tools (Kietzmann et al., 2020). These tools reduce technical barriers and allow non-experts to create synthetic content quickly. While such accessibility supports creative and commercial innovation, it also increases the risk of misuse, particularly in the areas of misinformation, identity theft, harassment, scams, and reputational attacks (Westerlund, 2019).

Legal Risks of Synthetic Media and Deepfakes

Synthetic media creates several legal risks. First, deepfakes may be used to spread misinformation and disinformation. A manipulated video of a political leader, public figure, or institutional representative may create confusion, influence public opinion, and undermine trust in official information. This is especially concerning during elections, public crises, or sensitive national issues (Chesney & Citron, 2019).

Second, deepfakes may violate privacy and personal autonomy. A person's face, voice, or identity can be used without consent to create misleading or harmful content. This raises legal concerns about personality rights, consent, dignity, and protection against identity exploitation. Non-consensual deepfake content may also cause emotional distress, reputational damage, and social harm to victims (Citron, 2014; Franks & Waldman, 2019).

Third, deepfakes may create difficulties in defamation law. If synthetic media falsely portrays a person as saying or doing something damaging, the victim may suffer reputational harm (Chesney & Citron, 2019). Legal action may nevertheless be difficult when the creator is anonymous, the content is distributed across multiple platforms, or the manipulated material spreads rapidly before it can be removed. Existing remedies may therefore operate more slowly than the circulation of the harmful content itself (Westerlund, 2019).

Fourth, deepfakes raise concerns about digital evidence. As synthetic media becomes more realistic, courts and enforcement agencies may face challenges in determining whether video or audio evidence is authentic. This may affect investigations, trials, and public trust in digital evidence. According to Chesney and Citron (2019), this component of the broader “liar’s dividend,” where people may reject authentic and real evidence by claiming that it was generated by artificial intelligence, AI.

These legal risks show that synthetic media regulation requires laws that are clear, specific, and adaptive. General digital laws may address some consequences of deep-fake misuse, but they may not fully cover the technological complexity and speed of AI-generated media.

International Policies and Legal Perspectives

As the rapid evolution of generative artificial intelligence intensifies concerns over misinformation and media integrity, governments worldwide have begun introducing regulatory and policy measures to address the risks posed by synthetic media and deepfake technologies. These regulatory responses reflect a growing recognition that technological advancement alone is insufficient to manage the societal implications of AI-generated content, particularly in maintaining accountability, transparency, and public confidence in media systems.

Internationally, the European Union (EU) has taken a leading role through the Artificial Intelligence Act, which adopts a risk-based regulatory approach and includes transparency obligations for certain AI-generated or manipulated content (European Parliament & Council of the European Union, 2024). Other regulatory approaches have similarly emphasised disclosure, labelling, platform responsibility, and accountability for harmful uses of synthetic media (Chesney & Citron, 2019). These approaches illustrate a shift from relying only on general legal remedies toward rules that address risks created specifically by AI-generated content.

Within Southeast Asia, Singapore provides a useful regional benchmark for policy readiness. The Protection from Online Falsehoods and Manipulation Act 2019 (POFMA) provides mechanisms such as correction directions and, in specified circumstances, measures that restrict access to false statements of fact in the public interest (Protection from Online Falsehoods and Manipulation Act 2019). Although POFMA is not a deep-fake-specific law, it demonstrates a more direct regulatory response to online falsehoods than reliance solely on general legal provisions. Singapore’s broader AI-governance approach also illustrates how legal measures can operate alongside governance guidance and transparency principles.

Despite differences in regulatory intensity and enforcement mechanisms, these international and regional approaches share a common emphasis on transparency, platform responsibility, and institutional oversight. Collectively, they illustrate how legal and policy interventions are

being used to address the challenges posed by synthetic media and to restore confidence in digital information ecosystems. These global and regional developments provide important comparative benchmarks for assessing Malaysia's policy readiness in regulating synthetic media and deepfakes.

Malaysia's Existing Legal Framework

Currently, in Malaysia, there have not been a single law dedicated entirely to synthetic media or deepfakes. Instead, different legal instruments may become relevant depending on the conduct and harm involved. The Communications and Multimedia Act 1998 (CMA 1998), including Sections 211 and 233, may be relevant to certain harmful communications distributed through network services. These provisions are not deepfake-specific; their relevance depends on the nature of the communication and the applicable statutory elements (Communications and Multimedia Act 1998).

The CMA 1998 was enacted before modern generative AI became widely available and does not expressly define synthetic media, deepfakes, AI-generated impersonation, or manipulated digital identity. Consequently, deepfake-related cases may require application of broader content rules rather than a purpose-built statutory framework. The Defamation Act 1957 may be relevant when false synthetic content harms reputation, but defamation remedies are generally reactive because they operate after publication and injury have occurred. This limitation is especially significant where manipulated content spreads rapidly (Tan et al., 2023). The Evidence Act 1950 is relevant to the admissibility and treatment of documentary and computer-generated evidence. Deepfakes complicate the factual assessment of authenticity because realistic audio or video may require technical verification before its evidential reliability can be evaluated. As synthetic-media quality improves, investigators and courts may increasingly depend on authentication procedures and expert analysis (Verdoliva, 2020).

The Penal Code may become relevant when synthetic media forms part of conduct such as fraud, intimidation, extortion, or other criminal wrongdoing. However, the Code is not a statute specifically designed to regulate AI-generated manipulation. Liability therefore depends on whether the conduct satisfies the elements of an existing offence rather than on the mere use of deepfake technology (Penal Code (Act 574) Malaysia).

The Online Safety Act 2025 represents an important development in Malaysia's digital-governance framework by strengthening regulatory attention to harmful online content and platform responsibilities. It should not, however, be described as a law that specifically regulates deep fakes. Its significance for synthetic media lies in the extent to which platform duties, risk-management measures, reporting processes, and enforcement mechanisms can be applied to harms involving AI-generated or manipulated content. This distinction is important when assessing whether Malaysia has a general legal basis for intervention or a framework specifically designed for synthetic media (Online Safety Act 2025).

Overall, Malaysia's current legal framework provides a partial foundation for regulating synthetic media, but it remains fragmented. The absence of deepfake-specific legal provisions may limit the country's regulative readiness.

The Regulative Pillar: Legal Frameworks and Enforcement

This study is guided by Institutional Theory, specifically Scott's regulative pillar. According to Scott (2013), there are three main institutions, which are regulative, normative and cultural-cognitive. The regulative pillar concerns formal rules, laws, monitoring arrangements, enforcement mechanisms, and sanctions that shape and constrain behaviour. In this study, 'regulative readiness' refers to the extent to which Malaysia's formal legal framework, regulatory responsibilities, and enforcement arrangements are sufficiently clear, applicable, and capable of responding to harms associated with synthetic media and deepfakes. The focus is therefore not on social norms or public beliefs, but on the adequacy of formal legal and regulatory arrangements.

Applying the regulative pillar provides a structured basis for evaluating Malaysia's policy readiness. The assessment considers whether existing laws can be applied to synthetic-media harms, whether regulated conduct and responsibilities are clearly defined, whether enforcement can respond effectively to rapidly circulating content, and whether platform and evidentiary responsibilities are sufficiently specified. This theoretical lens therefore connects the study's legal analysis directly to the question of institutional readiness rather than treating 'readiness' as an undefined policy label (Scott, 2013).

Methodology

Research Design and Procedure

This study adopted a qualitative research design to examine Malaysia's legal and policy readiness in regulating synthetic media and deepfakes. A qualitative approach was considered suitable because the study aimed to explore expert views, legal concerns, and regulatory challenges related to emerging AI-generated media. Qualitative research is appropriate when a study seeks to understand meanings, experiences, and institutional perspectives in depth (Creswell & Poth, 2018).

The research procedure involved three main stages. The first stage was participant selection. Four participants were purposively selected because the study was exploratory and required cross-sector perspectives rather than statistical representation. Inclusion was based on professional experience directly relevant to at least one of the study areas: government communication, public relations, media law or media-industry content governance. The participants' professional roles were used to establish relevant expertise for the research questions. Because the study needed information-rich participants with practical or specialized understanding of media regulation, communication governance, and legal concerns, purposeful sampling was acceptable (Palinkas et al., 2015).

The second stage was data collection. Semi-structured interviews were conducted to obtain participants' views on existing legal frameworks, enforcement challenges, legal gaps, platform responsibility, and policy readiness in addressing deepfakes. Semi-structured interviews allowed comparable questions across participants while providing flexibility to explore sector-specific experiences (Kallio et al., 2016). Document analysis was conducted to triangulate and contextualise the interview findings. The documents examined comprised Malaysian legislation and official policy or governance materials directly relevant to online content, reputation, digital evidence, criminal misuse, platform responsibility, and AI governance,

including the Communications and Multimedia Act 1998, Communications and Multimedia (Amendment) Act 2025, Defamation Act 1957, Evidence Act 1950, Penal Code, Online Safety Act 2025, and National Guidelines on AI Governance and Ethics. Materials in force or publicly available up to 2026 were selected purposively for their direct relevance to the study objective. Document analysis is appropriate for examining official records and policy texts that support qualitative interpretation (Bowen, 2009).

The third stage was data analysis. Interview data were analysed using thematic analysis, with attention to recurring patterns concerning legal adequacy, definitional clarity, enforcement limitations, platform responsibility, and reform priorities. The document analysis was compared against these interview themes to identify areas of convergence, qualification, or legal context. Interpretation was guided by the regulative pillar of Institutional Theory (Scott, 2013). The analysis was conducted using familiarization, coding, theme development, review and reporting methodology as described by Braun and Clarke (2006). Given the exploratory four-participant design, the study does not claim statistical generalisability; its purpose is to develop a cross-sector qualitative assessment of regulative readiness.

Participants

Four participants were purposively selected based on professional roles that provided direct relevance to media governance and synthetic-media regulation. The sample was intentionally small because the study sought focused, information-rich perspectives across four sectors: government communication, public relations, media law, and media-industry content governance. The four-participant design is therefore treated as an exploratory cross-sector sample, and the findings are interpreted together with documentary evidence rather than presented as representative of all Malaysian stakeholders.

Table 1: Participant Profiles

Participant	Professional Background
P1	Government Communication Officer (Jabatan Penerangan Malaysia)
P2	Public Relations Practitioner
P3	Media Law Academician
P4	Former Media Industry Practitioner (Content Review and Censorship Division, ASTRO)

The selected participants provided complementary perspectives from government communication, public relations, academia, and media-industry practice. This cross-sector composition strengthened the exploratory design by allowing the legal framework to be considered from regulatory, communication, legal, and operational viewpoints. Interview findings were triangulated with the documentary analysis to support the assessment of Malaysia's regulative readiness.

Ethical Compliance

The ethical research guidelines for studies involving human subjects were followed in the conduct of this research. Prior to data collection, participants were made aware of the study's objectives. Their participation was entirely voluntary, and their informed consent was acquired. In these regards, codes (p1-p4) were used to anonymize participant identities and the data gathered was solely utilized for academic purposes. Throughout the research process, confidentiality was maintained and kept.

Findings and Discussion

The thematic analysis generated four interrelated themes: (1) fragmented legal coverage that provides only a partial legal basis; (2) definitional uncertainty because synthetic media and deepfakes are not clearly specified in existing laws; (3) reactive and enforcement-limited regulation, including difficulties in tracing sources and responding at platform speed; and (4) the need for clearer platform accountability and AI-specific legal safeguards. These themes are discussed through the regulative pillar of Institutional Theory (Scott, 2013).

Existing Laws Provide a Partial Legal Basis

The findings show that Malaysia has several existing laws that may be applied to deepfake related harms. Participants acknowledged that current legal instruments, particularly the Communications and Multimedia Act 1998, provide a foundation for addressing harmful online content. Other laws such as the Defamation Act 1957, Evidence Act 1950, and Penal Code may also be relevant depending on the nature of the case.

As noted by Participant 4:

"I think existing laws can address some consequences of misuse, but they don't specifically address deepfakes. Regulations tend to react after harm occurs rather than preventing the issue in the first place."

Similarly, Participant 3 emphasised the challenge of keeping legislation aligned with technological developments:

"Technology develops much faster than regulation, so policymakers are often trying to catch up."

These findings indicate the presence of regulatory gaps in Malaysia's current governance framework. Although initiatives such as the Online Safety Act 2025 represent positive developments, participants suggested that clearer legal definitions and AI-specific provisions remain necessary. This finding supports Chesney and Citron (2019), who argued that legal systems often experience regulatory lag when responding to emerging technologies. From the perspective of Institutional Theory, this reflects limitations within the regulative pillar, where formal rules and enforcement mechanisms have yet to fully adapt to synthetic media developments (Scott, 2013).

Absence of Clear Deepfake-Specific Legal Definitions

A major finding of this study is the lack of clear legal definitions for synthetic media and deepfakes. Participants indicated that without specific legal terminology, enforcement may become difficult and inconsistent.

Participant 3 stated:

“Previously, most legal concerns focused on traditional online content, but now we have technologies that can generate realistic videos, audio, and images that are difficult to distinguish from genuine content. So, this creates new legal questions about things like authenticity, accountability, even consent. The challenge is that technology develops much faster than regulation, so policymakers are often trying to catch up.”

This reflects the issue of regulatory lag, where technological development moves faster than legal reform. In the context of deepfakes, the absence of legal definitions creates several problems. First, it may be unclear whether a law applies to AI-generated images, voice cloning, manipulated videos, or fully synthetic content. Second, the law may not clearly distinguish between harmful deepfakes and legitimate uses such as satire, education, parody, or entertainment. Third, enforcement agencies may face difficulty determining whether an offence has occurred if the law does not clearly define the regulated conduct.

Participant 2 also highlighted the issue of legal clarity by stating:

“One of the biggest challenges is actually the fact that deepfake and synthetic media are still quite new, so the legal side is still trying to catch up. First, there’s the issue of clarity. Sometimes it’s not very clearly defined under existing law, so it becomes complicated to classify and take action specifically for deepfake-related cases.”

This shows that the absence of specific definitions does not only affect legal interpretation but also practical enforcement. If deep-fake-related harm is not clearly classified under existing law, agencies may face difficulties determining the appropriate legal route. This may delay action and create uncertainty for victims, regulators, platforms, and legal practitioners.

Clear definitions are important because they determine the scope of regulation. For example, a legal definition of deepfake should include AI-generated or AI-manipulated content that falsely represents a person’s appearance, voice, speech, or actions. At the same time, the definition should be carefully drafted to avoid overregulation of harmless or creative content.

This finding supports Tan et al. (2023), who highlight that deep-fake technology creates legal uncertainty in relation to identity, consent, and personal protection. Without specific legal definitions, victims may face difficulties seeking remedies, and enforcement agencies may rely too heavily on broad interpretation of existing laws.

Regulation Remains Largely Reactive

The findings also show that Malaysia’s current legal response to deepfakes is largely reactive. Existing laws tend to operate after harmful content has been created, distributed, and reported.

This creates a major challenge because deepfake content can spread quickly through social media and messaging platforms.

According to Participant 4:

“Regulations tend to react after harm occurs rather than preventing the issue in the first place.”

Participant 2 also highlighted the importance of digital literacy initiatives:

“In real situations, speed is a big issue. In PR itself, we see that once something is uploaded online, it can spread very quickly. Even before investigation or enforcement takes place, the content may already have reached a wide audience. And that’s where reputational impact happens fast.”

Participant 1 gave a practical example of how false or AI-generated content may affect public communication:

“Kadang-kadang yang pasal isu minyak tu, ada orang buat semua poster based on AI, pakai AI lah. Kadang-kadang dia sebar lagi cepat daripada apa yang dia sampaikan.”

This statement shows how AI-generated content can spread faster than official clarification. In the context of government communication, this creates pressure on agencies to counter misinformation quickly. It also highlights why legal frameworks should not only punish harmful content after the fact but also support faster reporting, takedown, and verification mechanisms.

The need for preventive regulation is consistent with international developments. Moreover, transparency requirements under the European Union's Artificial Intelligence Act mandate the disclosure of specific content created or altered by AI (European Parliament & Council of the European Union, 2024). This type of approach may help reduce deception by informing users when content is artificially generated or manipulated.

From the regulative pillar perspective, readiness is not only about punishing offenders after harm occurs. It also involves creating rules that reduce the risk of harm before it spreads. Therefore, Malaysia’s current framework requires further development to become more preventive and adaptive.

Enforcement Challenges, Source Tracing, and Platform Responsibility

The findings indicate that enforcement remains a major challenge in regulating deepfakes. Even when laws exist, enforcement may be difficult because synthetic media can be created anonymously, distributed rapidly, and hosted on platforms located outside Malaysia. This creates jurisdictional and technical challenges for local regulators. Participant 2 explained: “The third one is tracing the source. A lot of this content is either anonymous or uploaded from outside jurisdictions. So it’s not always straightforward to take immediate action.”

This finding is important because deep-fake-related offences are not always limited to domestic actors. A manipulated video may be produced outside Malaysia, uploaded using anonymous

accounts, and circulated through multiple platforms. This creates difficulties in identifying the original creator, proving intent, preserving evidence, and taking enforcement action.

Deepfake cases may involve multiple actors, including the creator, uploader, platform provider, content sharer, and algorithmic recommendation system. This makes it difficult to determine liability. If the creator cannot be identified, enforcement agencies may need to rely on platform cooperation to remove the content or provide relevant information.

Participant 1 emphasised the importance of cooperation with platform providers:

“Kalau kata benda tu dari peringkat penyedia platform tu sendiri boleh terus menurunkan benda-benda yang macam tu, saya rasa itu kerjasama yang sangat baik lah yang kerajaan boleh buat.”

This indicates that platform responsibility is a key issue in legal readiness. Social media companies, video-sharing platforms, and messaging services are often the main channels through which deep-fake content spreads. Without clear legal duties for platforms, harmful synthetic media may remain online for too long or continue circulating through reposts and private sharing. This issue is consistent with broader debates on platform governance, where online intermediaries are increasingly expected to take responsibility for harmful content circulation (Gillespie, 2018).

The Online Safety Act 2025 may provide an important basis for strengthening platform accountability. However, further clarity is needed regarding how platforms should handle AI-generated misinformation, deepfake impersonation, synthetic identity misuse, and harmful manipulated content. Platform duties may include rapid response to complaints, content removal, evidence preservation, transparency reporting, and cooperation with enforcement agencies.

At the same time, platform regulations must be balanced with freedom of expression. Overly broad rules may lead to excessive content removal or censorship. Therefore, Malaysia needs clear procedures that allow harmful deepfake content to be addressed quickly while protecting legitimate expression, satire, journalism, and creative content.

Need for AI-Specific Legal Reform

Participants consistently emphasized the need for clearer and more adaptive legal frameworks. Participant 3 stated:

“I would recommend clearer legal definitions, stronger disclosure requirements for AI generated content and greater investment in like institutional capacity. Policymakers should also work closely with technical experts, industry players and academics to ensure that regulatory approaches remain practical and adaptable as technology evolves.”

Participant 2 also explained:

“Moving forward, I think the most important strategy is to take a balanced approach, combining regulation, education, and technology. On the regulatory side, I think Malaysia

needs frameworks that are more adaptive to AI development so that the policies can evolve alongside technology.”

Participant 4 similarly stated:

“I think we need clearer policies, stronger institutional capacity and better public awareness. Media organisations should also establish internal protocols for handling suspected AI generated content. At the same time, regulatory agencies should continue updating their frameworks to keep pace with technological developments.”

These findings show that Malaysia requires legal and policy frameworks that are capable of evolving alongside AI technologies. This does not necessarily require a completely separate deepfake law. Legal reform may involve amendments to existing laws, new regulations under current legislation, or detailed guidelines with legal authority.

The findings suggest that Malaysia’s legal reform should focus on several areas. First, legislation or legally authoritative guidance should define ‘synthetic media’ and ‘deepfake’ in a technologically neutral manner. Second, the framework should distinguish harmful uses from legitimate uses such as satire, education, journalism, and creative production. Third, disclosure or provenance requirements should be considered for materially deceptive AI-generated or AI-manipulated content. Fourth, liability should be clarified across creators, uploaders, distributors, and platform providers according to their role and level of knowledge or control. Fifth, faster reporting and takedown procedures should be paired with evidence-preservation requirements and safeguards for freedom of expression. Sixth, evidentiary procedures should support authentication of disputed audio-visual material, while victim remedies should address impersonation, non-consensual synthetic media, reputational harm, and related misuse.

Participant 3 also warned against overregulation:

“We don’t want to over-regulate because AI can bring genuine benefits in education, entertainment, and creative industries. At the same time, there must be safeguards against harmful uses. The key is proportional regulation that targets harmful conduct without unnecessarily restricting legitimate expression.”

This point is significant because legal readiness should not only focus on control and punishment. It must also maintain space for innovation, education, satire, creative expression, and legitimate AI use. Therefore, Malaysia’s regulatory approach should be proportional, riskbased and targeted toward harmful conduct.

These reforms are important because synthetic media challenges traditional legal assumptions about authorship, identity, evidence, and responsibility. As Mirsky and Lee (2021) explain, deep-fake technology is not merely a technical issue but also a social and security concern because of its potential to deceive individuals and institutions. Therefore, Malaysia’s regulative readiness depends on the ability of its legal system to move beyond general digital regulation toward AI-specific legal clarity.

Overall, the findings indicate that Malaysia demonstrates partial regulative readiness. Existing laws provide a legal foundation, but clearer definitions, faster enforcement mechanisms,

platform accountability, digital evidence procedures, and AI-specific legal safeguards are needed to strengthen Malaysia's response to synthetic media and deepfake technologies.

Conclusion

This study examined Malaysia's policy readiness for synthetic media and deepfake regulation through Scott's regulative pillar of Institutional Theory. The findings indicate partial regulative readiness. Malaysia already has legal instruments that may address particular consequences of deepfake misuse, but the framework remains fragmented because these laws were not designed specifically for synthetic media. The main limitations identified were definitional uncertainty, reactive enforcement, difficulties in source tracing and cross-platform response, unclear allocation of platform responsibility, and the absence of sufficiently specific rules for disclosure, liability, and digital-evidence authentication. The study therefore does not conclude that Malaysia lacks regulation; rather, it finds that existing regulation requires clearer AI-specific application and stronger enforcement coordination. A proportionate approach is recommended so that harmful deception, impersonation, and non-consensual uses can be addressed without unnecessarily restricting legitimate creative, educational, journalistic, or satirical uses of AI. As an exploratory qualitative study based on four cross-sector participants and documentary analysis, the findings are not statistically generalisable, but they provide an evidence-based basis for further legal research and policy development in Malaysia.

-
- Acknowledgements:** The authors would like to acknowledge the School of Multimedia Technology and Communication, Universiti Utara Malaysia, for its academic support. The authors also thank the participants who contributed their time and perspectives to this research.
- Funding Statement:** No Funding. This research received no external financial support from public, commercial, or non-profit funding bodies.
- Conflict of Interest Statement:** The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Law, Government and Communication (IJLGC).
- Ethics Statement:** This study involved human participants and was conducted in accordance with ethical research standards. Informed consent was obtained from all participants prior to data collection. Participation was voluntary, participants were informed of the purpose and nature of the study, and identities were anonymised in the manuscript using participant codes. Data were used solely for academic purposes and handled confidentially. If the study received formal institutional ethics approval, the name of the approving committee and approval number should be inserted here before final submission.
- Author Contribution Statement:** All authors contributed significantly to the development of this manuscript. The first author was responsible for the conceptualisation, literature review, research design, data collection, analysis, and initial drafting of the manuscript. The second author provided academic supervision, methodological guidance, critical review, and substantive revision. Both authors reviewed and approved the final version of the manuscript and agreed to be accountable for the integrity of the work.
-

References

- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *U.C. Davis Law Review*, 51(2), 399–435.
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>
- Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
- Communications and Multimedia Act 1998 (Act 588) (Malaysia).
- Communications and Multimedia (Amendment) Act 2025 (Act A1743) (Malaysia).
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Defamation Act 1957 (Act 286) (Malaysia).
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- Evidence Act 1950 (Act 56) (Malaysia).
- Farid, H. (2022). Creating, using, misusing, and detecting deep fakes. *Journal of Online Trust and Safety*, 1(4). <https://doi.org/10.54501/jots.v1i4.56>
- Franks, M. A., & Waldman, A. E. (2019). Sex, lies, and videotape: Deep fakes and free speech delusions. *Maryland Law Review*, 78(4), 892–898.
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27, 2672–2680.
- Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12), 2954–2965. <https://doi.org/10.1111/jan.13031>
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Ministry of Science, Technology and Innovation. (2024). *National guidelines on artificial intelligence governance and ethics*. Government of Malaysia.
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1–41. <https://doi.org/10.1145/3425780>
- Online Safety Act 2025 (Act 866) (Malaysia).
- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533–544. <https://doi.org/10.1007/s10488-013-0528-y>
- Penal Code (Act 574) (Malaysia).

Protection from Online Falsehoods and Manipulation Act 2019 (Singapore).

- Ramteke, V., Babu, M., & Verma, P. (2024). Technology trends in synthetic media – Bibliometric analysis of existing literature and future scope. 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), 1–6. <https://doi.org/10.1109/ICIPTM59628.2024.10563652>
- Sahak, S., Rajamanickam, R., & Hassan, M. S. (2025). The limitation of freedom of expression by online media in Malaysia: Analysis of legal precedents. *Edelweiss Applied Science and Technology*, 9(9), 296–308. <https://doi.org/10.55214/2576-8484.v9i9.9801>
- Scott, W. R. (2013). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). SAGE Publications.
- Tan, Z. K., Chong, S. Z., Kuek, C. Y., & Tay, E. S. (2023). Individual legal protection in the deepfake technology era. *Advances in Social Science, Education and Humanities Research*, 119–129. https://doi.org/10.2991/978-2-38476-154-8_7
- Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). DeepFakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, 64, 131–148. <https://doi.org/10.1016/j.inffus.2020.06.014>
- Verdoliva, L. (2020). Media forensics and deepfakes: An overview. *IEEE Journal of Selected Topics in Signal Processing*, 14(5), 910–932. <https://doi.org/10.1109/JSTSP.2020.3002101>
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52. <https://doi.org/10.22215/timreview/1282>