**INTERNATIONAL JOURNAL
OF LAW, GOVERNMENT
AND COMMUNICATION
(IJLGC)**www.gaexcellence.com/ijlgc**DEEPPAKE TECHNOLOGY AND CYBER HARM:
A CONCEPTUAL FRAMEWORK LINKING LEGAL
REGULATION, ETHICAL COMPLIANCE, AND SOCIAL
PROTECTION**

Mohd Zulharmey Abdullah^{1*}, Siti Khadijah Abdullah Sanek², Irma Kamarudin³, Nur Irinah Mohamad Sirat⁴, Nurul Mazrah Manshor⁵

¹Faculty of Law, Universiti Teknologi MARA Cawangan Kedah, Kampus Sungai Petani, Malaysia

 zulharmey511@uitm.edu.my

 <https://orcid.org/0009-0008-1529-5610>

²Faculty of Law, Universiti Teknologi MARA Cawangan Kedah, Kampus Sungai Petani, Malaysia

 khadijah016@uitm.edu.my

 <https://orcid.org/0009-0000-2454-2179>

³Faculty of Law, Universiti Teknologi MARA Cawangan Kedah, Kampus Sungai Petani, Malaysia

 irma@uitm.edu.my

 <https://orcid.org/0009-0002-3312-5865>

⁴Faculty of Law, Universiti Teknologi MARA Cawangan Kedah, Kampus Sungai Petani, Malaysia

 irinah@uitm.edu.my

 <https://orcid.org/0009-0007-3860-7931>

⁵Faculty of Law, Universiti Teknologi MARA Cawangan Kedah, Kampus Sungai Petani, Malaysia

 mazrah@uitm.edu.my

 <https://orcid.org/0009-0001-0163-0755>

*Corresponding Author

Article Info:**Article history:**

Received date: 30.07.2026

Revised date: 24.08.2026

Accepted date: 10.09.2026

Published date: 22.09.2026

To cite this document:

Abdullah, M. Z., Abdullah Sanek, S. K., Kamarudin, I., Sirat, N. I. M., & Manshor, N. M. (2026). Deepfake Technology and Cyber Harm: A Conceptual Framework Linking Legal Regulation, Ethical Compliance, And Social Protection.

Abstract:

The rapid development of artificial intelligence (AI) has accelerated deepfake technology, which offers new creative possibilities but also raises significant ethical, legal and social issues. The growing misuse of deepfakes as for identity theft, misinformation, cyber harassment, financial fraud, electoral manipulation, and intellectual property infringement has exposed serious deficiencies in current legal systems, which remain fragmented, reactive, and inadequate to address the evolving nature of AI-generated cyber harms. Previous studies have looked at the ethical and legal issues of deepfake technology separately, but few have brought these together into an overarching governance framework to clarify the function of legal regulation in enhancing social protection. Therefore, this study is intended to construct a conceptual framework that connects legal regulation, ethical compliance, and social protection to lessen the adverse effects of deepfake technology in digital environments. The study adopted a narrative review methodology to critically synthesise multidisciplinary literature from the Scopus database on law, artificial intelligence, ethics, cybersecurity, governance and public policy. Thematic analysis of the study identifies

International Journal of Law, Government and Communication, 11(45), 630-649.

three key concepts, namely legal regulation, ethical compliance and social protection, that were integrated into a theoretically grounded framework based on AI Governance Theory. The findings show that statutory regulation is not enough to effectively regulate deepfake technology. Instead, ethical compliance is conceptualised as a mediating mechanism that promotes accountability, transparency, fairness, responsible AI development and institutional governance, thereby increasing the effectiveness of legal regulation and ultimately improving social protection from cyber-related risks. The study contributes to the theoretical framework of AI Governance Theory by integrating ethical and legal governance procedures into a single conceptual paradigm. Practically, it provides guidance to legislators, regulators, technology developers, digital platforms and policymakers who wish to develop comprehensive governance strategies to increase digital trust, protect fundamental rights and improve society's resilience to the risks posed by deepfake technology.

DOI: 10.35631/IJLGC.1145040

Keyword:

AI Governance; Deepfake Technology; Ethical Compliance; Legal Regulation; Social Protection;



© 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 ijlgc@gaexcellence.com.

Introduction

Deepfakes are a sophisticated form of synthetic media that have emerged as a consequence of the rapid development of artificial intelligence which has revolutionised the creation, manipulation and distribution of digital information. Deepfake technology can generate realistic images, audio and video that are often indistinguishable from real recordings. It's powered by algorithms based on deep learning called generative adversarial networks (GANs). Although technology has been a boon for digital innovation, healthcare, education and entertainment, its misuse has been a growing global concern. The spread of harmful deepfakes has facilitated identity theft, non-consensual intimate imagery, financial fraud, political disinformation, cyber harassment, and reputational damage, presenting modern societies with unprecedented ethical and legal challenges (Khanal & Koirala, 2026; Kukreti et al., 2026). These developments have raised more academic and regulatory debates on whether existing legal mechanisms can continue to protect fundamental rights in an era where digital deception undermines public trust in the truthfulness of information (Shakil & Mekuria, 2024). "Deepfake technology is not just a technological innovation but a complex governance issue that necessitates integrated legal, ethical and technological responses."

The various legal implications of deepfake technology have been well explored in previous work. One of the major concerns is privacy violations, based on recent research. Deepfakes

often use biometric data without the knowledge or consent of an individual, revealing gaps in existing privacy laws including the General Data Protection Regulation (GDPR) and other national data protection laws (Kishwar et al., 2025; Verma, 2024). Beyond privacy, deepfakes have become powerful tools for spreading false information, influencing elections, damaging reputations and undermining democratic integrity. Therefore, the defamation and electoral governance laws are facing a major obstacle (Khanal & Koirala, 2026; Roy et al., 2026; Soneca, 2025). The emergence of AI-generated work has also raised new challenges for intellectual property law regarding authorship, ownership, and copyright infringement (Khare & Raghuwanshi, 2025; Kim, 2025). Increasing evidence also suggests that juveniles are being exploited through identity manipulation and deepfake pornography, which highlights the substantial gaps in child protection legislation in many jurisdictions (Boparai et al., 2026; Okolie, 2023). Therefore, countries such as the US, EU, China, and India have adopted various regulatory measures such as criminal sanctions, tort liability, transparency requirements through the EU Artificial Intelligence Act, and platform liability (Bień-Węćowska, 2025; Kadri & West, 2025; Kishwar et al., 2025; Perriello, 2026). However, these legal solutions are scattered, jurisdictional and primarily reactive to advances in technology.

There is a specific conceptual gap despite a growing body of literature on the legal and ethical implications of deepfake technology. The bulk of existing legal scholarship focuses on the adequacy of statutory provisions, regulatory solutions, liability, privacy, defamation, intellectual property, cybercrime and platform responsibility, often within specific jurisdictions (Kadri & West, 2025; Kakkar & Nandrajog, 2025; Perriello, 2026). Ethical studies, however, are more likely to focus on principles such as transparency, accountability, fairness, informed consent, human dignity, and responsible AI practices. While providing significant insights into the legal and ethical challenges of deepfakes, these studies largely treat the legal regulation and ethical governance as separate dimensions, rather than as a dynamic interaction in an integrated governance process. More concretely, existing research provides little conceptual explanation of the mechanism through which legal regulation translates into ethical compliance among governments, technology developers, digital platforms and other relevant stakeholders, and how such compliance in turn contributes to social protection against deepfake-related cyber harms. Thus the question inadequately addressed is not simply the existence or adequacy of legal and ethical responses, but the governance mechanism that connects formal legal regulation with practical ethical behaviour and, ultimately, with social protection. This study fills this gap by proposing a conceptual framework with legal regulation as the independent variable, ethical compliance conceptualised as a mediating mechanism and social protection as the final governance outcome. The study offers an integrated governance perspective that links legal regulation to the wider goal to safeguard people, communities, and democratic institutions from cyber related risks caused by deepfakes by framing ethical compliance as the channel through which legal obligations are translated into responsible AI practices. The framework is conceptual and does not empirically test these relationships but provides theoretically grounded propositions to guide future empirical research and policy development.

The proposed conceptual framework makes several important contributions to the growing research on cyber law, digital ethics, and AI governance. First, it advances research by integrating ethical compliance and legal regulation into a unified analytical model, which goes beyond the current fragmented doctrinal debates to provide a more comprehensive governance perspective. Second, the framework considers social protection, which includes the protection of individual dignity, privacy, democratic integrity, public trust and digital security, as the ultimate regulatory objective. Third, the study adopts a governance position that corresponds

to the current debate on AI regulation that is progressively recognising that legislative measures alone are not enough to address technological risks and there is a need for institutional accountability with ethical principles, technological safeguards and collaborative governance by governments, businesses, civil society and international organisations (Hanna et al., 2026; Kishwar et al., 2025; Shakil & Mekuria, 2024). The conceptual framework is built on the concepts of AI governance and responsible innovation, where transparency, accountability, justice, human rights protection and regulatory compliance are considered as essential pillars for trustworthy AI ecosystems. These perspectives collectively provide a sound theoretical basis to study the interaction between ethical and legal structures in reducing the cyber harm of deepfake technology.

The rest of the study is structured as follows. The literature on deepfake technology, cyber damage, legal regulation, ethical compliance and social protection is reviewed in the text that follows this introduction. The theoretical justification of the suggested relationships is discussed in the next section, as is the development of the conceptual framework and relevant research proposals. The study then discusses the practical and policy implications of the framework for legislators, regulatory bodies, technology companies, digital platforms and other stakeholders responsible for AI governance. The study concludes with a summary of the study's contributions, a discussion of its conceptual limitations, and recommendations for future empirical research to validate and extend the proposed framework in different legal and regulatory environments.

Literature Review

Legal Regulation

Legal regulation is the primary institutional mechanism for addressing the growing concerns about deepfake technology today. The rapid development of AI-generated synthetic media has tested the effectiveness of traditional legal theories, especially in aspects related to privacy, defamation, fraud, election integrity, copyright infringement, and cybercrime (Kukreti et al., 2026). Comparative data reveals marked differences in regulatory responses across jurisdictions. Some US jurisdictions have introduced criminal offences, civil remedies and tort-based procedures to address the harm from deepfake development and transmission. But, modern tort principles encounter real-world hurdles in ascertaining the fault of unknown wrongdoers, apportioning liability, and controlling the dissemination of modified material via viral pathways (Kadri & West, 2025). In contrast, the Artificial Intelligence Act, which treats deepfakes as “limited-risk” artificial intelligence systems, and thus, imposes transparency obligations for the proper labelling of content produced by AI, is a more holistic regulatory approach adopted by the European Union (Bień-Węęska, 2025; Perriello, 2026). Complementary laws like the General Data Protection Regulation (GDPR) and the Digital Services Act enhance protections for online misinformation, platform accountability, and personal data (Perriello, 2026). Furthermore, China has established some regulatory mechanisms focusing on transparency, traceability, and platform responsibility to prevent the abuse of synthetic media (Vinogradov & Kuznetsova, 2024). In contrast, India still largely depends on the Information Technology Act 2000 and other general criminal laws, which scholars argue are inadequate to deal with the emerging problems of AI-generated deception, misuse of digital identities and cross-border cyber-harm (Kakkar & Nandrajog, 2025; Singh et al., 2025). Deepfake technology presents significant challenges for intellectual property law beyond national legislation, as artificial intelligence systems can reproduce copyrighted works,

trademarks, voices and facial likenesses without authorisation. This has left questions of ownership, authorship and liability unanswered (Khare & Raghuwanshi, 2025; Kim, 2025). The overall literature shows that the existing legal systems are still fragmented, reactive and dependent on jurisdiction. This shows the need for uniform legal norms that could effectively protect human rights and the interests of society, balancing technological progress.

Ethical Compliance

Even when legal regulation sets baseline criteria for what activities are permissible, scholars increasingly argue that legal compliance is not enough to address the complex hazards associated with deepfake technology. Ethical compliance is an additional governance mechanism that promotes responsible AI development, deployment and use based on principles such as transparency, accountability, fairness, human dignity, informed consent, and respect for fundamental rights (Khanal and Koirala, 2026). One of the most significant ethical issues pointed out in the literature is privacy since deepfakes frequently utilise people's biometric information, facial images and voices without their consent, particularly in instances of non-consensual intimate imagery, identity theft and reputation attacks (Verma, 2024). The ethical issues that challenge democratic processes and social cohesion include privacy, algorithmic bias, manipulation of public opinion, political misinformation, and the erosion of trust in digital communications (Fernández et al., 2026; Khanal & Koirala, 2026). Moreover, vulnerable populations, especially women and children, are disproportionately susceptible to being targeted by harmful deepfakes, highlighting the moral obligation of governments, digital platforms, and technology developers to put in place stronger protective measures against misuse (Boparai et al., 2026). Hence, contemporary AI governance literature calls for ethical-by-design approaches, which integrate ethical standards into every stage of the AI system lifecycle, rather than treating them as optional post-development considerations. These approaches focus on algorithmic transparency, explainability, risk assessment, oversight by humans, and stakeholder accountability, which are all key elements of responsible AI governance (Fernández et al., 2026). Ethical compliance is therefore not only a normative ideal, but an operational governance mechanism that supports legal regulation by encouraging organisations to adopt higher standards of responsibility beyond legislative responsibilities. Thus, in the proposed conceptual framework, ethical compliance is conceptualised as the mediating mechanism that converts legal regulation into more effective governance outcomes that may reduce cyber harm caused by deepfake technology.

Social Protection

The ultimate goal of regulation of deep fake technology is not only law enforcement but also full social protection from the increasingly complex types of cyber damage. Social protection within the framework of digital governance is about safeguarding people, communities and democratic institutions from technology practices that threaten equality, privacy, security, dignity and public trust. The social implications of malicious deepfakes have been proven to be profound, such as identity theft, financial fraud, cyberbullying, online sexual exploitation, election interference, damage to reputation, and the proliferation of misinformation (Khanal & Koirala, 2026; Kukreti et al., 2026). In addition to eroding democratic legitimacy and social resistance to manipulated media, these effects also undermine trust in digital information ecosystems (Perriello, 2026). Academics are increasingly calling for a multi-layered governance strategy that includes ethical AI governance, legal reform, tech innovation, and public education to build a more resilient society to deepfake threats (Singh et al., 2025).

Technological interventions such as AI-based detection algorithms, blockchain-enabled content authentication, watermarking systems, and digital provenance verification have shown significant promise in bolstering law enforcement and content authenticity (Singh et al., 2025). However, without concerted cooperation between governments, tech firms, civil society organisations, academic institutions and international regulatory authorities, technological solutions alone will still be insufficient. Increasing public awareness and digital proficiency allows individuals to critically evaluate altered media and thus reduces their vulnerability to disinformation and deception (Khanal & Koirala, 2026). Thus, at the governance level, social protection is the desired outcome of an effective regulatory ecosystem, in which ethical compliance and legal regulation work together in an effort to reduce cyber harm, protect fundamental rights, defend democratic values and boost public trust in the digital environment. Therefore, social protection is conceptualised in this study as a dependent variable that indicates how well ethical and legal governance institutions respond to the problems caused by deepfake technology.

Methodology

Research Design

This study adopts a narrative review methodology to critically synthesise the body of research on ethical and legal implications of deepfake technology and produce a conceptual framework linking social protection, ethical compliance and legal regulation. Narrative reviews are useful for conceptual research as they enable the synthesis of multidisciplinary literature, aid in theory development and provide a holistic view of nascent issues where empirical evidence is still scanty (Baumeister & Leary, 1997; Snyder, 2019). Narrative reviews focus more on critical interpretation, conceptual integration and theory development than systematic reviews, which are mainly intended to address specific research topics by rigorous inclusion processes (Ferrari, 2015). Deepfake technology is affecting many areas, such as law, artificial intelligence, ethics, cybersecurity, governance, and public policy. A narrative review can be flexible to study many scholarly perspectives and find common themes across jurisdictions. The objective is not to empirically establish causal linkages but to critically synthesise the available information, identify conceptual gaps and suggest an integrated framework that can be used to guide future empirical research and policy formulation.

The review is organised around three major themes identified in the literature: legal regulation, ethical compliance and social protection. These concepts were selected because they are commonly discussed as key topics in discussions about deepfake regulation and AI governance. The narrative review method is particularly suitable for the achievement of the theoretical objectives of the present research as the conceptual model designed in this research is based on an interpretative analysis of the current literature, rather than statistical meta-analysis.

Key Steps in Conducting the Narrative Review

The narrative review was performed following a structured but flexible approach to enhance the validity, transparency, and completeness of the literature synthesis. The first step was to define the scope of the review. The research focus was set on the ethical and legal ramifications of deepfake technology, specifically regarding social protection, ethical compliance and legal regulation. Then, by combining the concepts of deepfake technology, artificial intelligence,

legal regulation, ethical compliance, AI governance, cyber damage, privacy, disinformation, social protection, and digital governance, relevant keywords and search strings were created.

The data collection was performed using the Scopus database, which is considered as one of the most comprehensive multidisciplinary indexing databases of peer-reviewed academic literature worldwide. Scopus was chosen for its extensive coverage of journals, strict indexing standards, citation tracking capabilities, and the presence of high-quality papers in the areas of public policy, computer science, law, information systems, and ethics. Preference was given to peer-reviewed journal articles, conference proceedings, book chapters, and review papers that addressed the ethical, legal, governance, and regulatory issues of deepfake technology. Recent articles were also preferred to ensure the assessment reflects the fast evolving nature of AI regulation and synthetic media technologies.

Papers found in the literature search were examined for their relevance based on their support for the aims of the study. Conceptual analyses did not include studies that were primarily focused on the technological development of algorithms without significant examination of the ramifications for governance, ethics, law or society. The selected literature was then subjected to theme analysis through iterative reading and comparison. At this stage, the identification of recurrent ideas, theoretical stances, regulatory approaches, governance systems and policy suggestions led to three broad topics of legal regulation, ethical compliance and social protection. The proposed conceptual framework has been developed on the basis of these concepts as an analytical basis.

Finally, the synthesised findings were critically analysed to identify gaps, inconsistencies and contradictions in the body of current knowledge. The review critically synthesised findings from many academic disciplines and jurisdictions, creating conceptual links between the three dimensions rather than merely summarising previous research. The integration made it possible to create the conceptual framework for the demonstration of the mediating role of ethical compliance in improving social protection through effective legal regulation. Beside adding to ongoing academic debates on AI governance, cyber law and responsible regulation of deepfake technology, the proposed approach provides a theoretical basis for future empirical validation.

Data Collection and Review Strategy

The data collection process used the Scopus database because of its wide coverage of high-quality peer-reviewed publications in several multidisciplinary fields such as law, artificial intelligence, cybersecurity, public policy, ethics and information systems. Scopus is regarded as one of the most reliable bibliographic databases to conduct conceptual and literature review investigations due to its extensive citation coverage, rigorous indexing criteria and the inclusion of internationally recognised publications. Deepfake technology is an interdisciplinary technology, and Scopus provides a proper forum for documenting current scholarly discussions on legal regulation, ethical governance, and societal implications. A structured search strategy was used to ensure that all relevant literature was captured. The search string was developed to maximise search sensitivity while maintaining relevance, using Boolean operators and conceptual elements of the study. The search term used was:

("deepfake" OR "deep fake" OR "synthetic media" OR "digital impersonation") AND ("legal" OR "law" OR "regulation" OR "legislation") AND ("framework" OR "policy" OR "guideline"

OR "structure") AND ("ethics" OR "liability" OR "responsibility" OR "accountability") AND ("privacy" OR "consent" OR "rights" OR "protection")

The search only considered peer-reviewed publications indexed in Scopus, including scholarly book chapters, journal articles, conference proceedings and review papers, that explored the ethical, legal, governance or policy aspects of deepfake technology. The assessment focused on recent publications on new regulations, AI governance, privacy protection, digital rights, accountability and cyber impact to ensure it captured current developments in artificial intelligence policy. The search excluded publications that focus solely on technical algorithm development or engineering performance, without regard to legal, ethical or governance issues, as these are outside the scope of the present conceptual analysis.

Relevant publications were retrieved, and an approach of integrative thematic analysis was used to synthesise the literature. Unlike descriptive narrative summaries, integrative thematic analysis helps researchers to critically compare findings across multiple fields, to identify recurring concepts, to analyse theoretical convergence and divergence, and to generate higher-order conceptual insights (Snyder, 2019; Torraco, 2005). This approach is very well-suited to emerging research domains, such as deepfake technology, in which knowledge is distributed across multiple academic disciplines and regulatory regimes. The assessment process involves reading, coding, comparing and interpreting the selected papers to identify recurring legal, ethical, governance and societal challenges of deepfake technology.

The thematic analysis process consisted of four iterative phases. First, the selected papers were read in depth in an effort to familiarise the researchers with the current knowledge and to identify recurrent problems. Second, the substantive content of relevant ideas, arguments and regulatory strategies was coded. Third, consistent cross-study comparison resulted in the groupings of related codes into larger conceptual categories. Finally, the categories were condensed into three overarching themes that form the basis of the proposed conceptual framework: legal regulation, ethical compliance, and social protection. The first theme is the formal legal systems, regulatory rules and statutory responses that govern deepfake technology. The second topic concerns moral values, accountability, transparency, organisational responsibility and responsible AI governance. The third theme encompasses wider social implications of good governance, including privacy protection, digital rights, democratic integrity, cybersecurity, and public trust.

The integrated thematic analysis facilitated a critical synthesis of existing knowledge, examining conceptual linkages between the three constructs, rather than merely summarising previous research. The analysis revealed that while the formal institutional framework for deepfake technology is established by legal regulation, the extent to which technology developers, digital platforms, regulatory bodies and users adhere to ethical principles has a significant impact on the technology's ability to reduce cyber harm. Therefore, the study provides the theoretical basis for developing the conceptual framework by using ethical compliance as the conceptualised mediating mechanism to enhance the protection of the society from the cyber harm created by deepfakes. This synthesis draws on prior research by incorporating diverse legal and ethical perspectives to offer a coherent view of governance that might inform empirical research and influence policy.

Key Findings from the Narrative Review

The narrative review revealed multiple common themes in the literature on governance of deepfake technology. Scholars have repeatedly pointed out that, despite the differences in legal approaches across governments, the existing regulatory processes are piecemeal and are unable to keep up with the rapid development of artificial intelligence. The research also shows that to reduce cyber harm and improve social protection, effective governance involves more than legal regulation, and requires technological innovation, ethical compliance and collaborative governance. The key conclusions are summarised in **Table 1**.

Table 1. Key Findings from the Narrative Review on Legal Framework and Deepfake Technology

Key Finding	Description
1. Deepfake technology presents multidimensional legal challenges	The legal risks of deepfake technology discussed in the literature are privacy violation, identity theft, defamation, misinformation, electoral manipulation, copyright infringement, financial fraud and cyber harassment. These harms impact persons, organisations and democratic institutions and indicate that deepfake governance is not just a matter of traditional cybercrime regulation but of wider issues of digital rights, human dignity and public trust.
2. Existing legal frameworks remain fragmented and reactive	Most jurisdictions rely on existing laws on privacy, defamation, copyright, cybercrime and data protection, rather than specific laws on deepfake technology. These laws provide some protection, but often do not cover anonymous offenders, cross-border spread, AI generated synthetic media and rapidly evolving technology. So the legal responses are not pre-emptive but reactive.
3. Regulatory approaches vary considerably across jurisdictions	The comparative analysis shows the significant difference in the legal regulation. The AI Act is a step toward EU's holistic governance approach including GDPR and Digital Services Act with a focus on transparency and platform accountability. The US's dependence on state tort law, criminal sanctions and civil remedies leads to regulatory inconsistency. China stresses traceability, transparency and platform accountability. India continues its heavy reliance on general cyber and criminal laws. That means there are no specific deepfake laws.
4. Privacy protection emerges as the dominant legal concern	The most widely discussed issue throughout the literature is privacy breaches. Biometric data, facial images, voice recordings and other personal data are also often misused by deepfakes without informed consent. Scholars have highlighted the increase in non-consensual intimate imagery, identity impersonation and digital exploitation and exposed the shortcomings of existing privacy laws and data protection mechanisms.

5. Ethical compliance complements legal regulation	The review suggests that legal compliance is not sufficient to effectively regulate deepfake technology. Complementary governance mechanisms are ethical principles such as transparency, accountability, fairness, explainability, oversight by humans, informed consent and responsible AI development. Ethical compliance also encourages organisations and technology developers to go above and beyond minimum legal requirements and to prevent cyber harm before the law has to step in.
6. Intellectual property law faces emerging challenges	It is hard to think about copyright ownership, authorship, originality, trademark protection, and personality rights in the old ways, given the growing incidence of AI-generated synthetic media. Legislative reforms are needed to address content produced by AI and keep pace with the rapidly evolving AI generative technology as there is little guidance under current intellectual property laws.
7. Vulnerable groups require enhanced legal protection	Malicious deepfakes can be disproportionately threatening to women, children, public figures and those who are digitally vulnerable, particularly when compared to non-consensual pornography, online exploitation, cyberbullying, identity theft and reputational attacks. The literature consistently supports strengthening child protection measures, victim-centred remedies and criminal sanctions to protect vulnerable populations.
8. Technological solutions strengthen legal enforcement	AI-based detection systems, blockchain authentication, digital watermarking, provenance verification and content authentication are increasingly seen as important tools in supporting legal enforcement. Nevertheless, scholars stress that technological solutions cannot substitute for legal regulation, because detection technologies alone are not enough to deal with questions of accountability and liability.
9. Collaborative governance is essential for effective regulation	Good governance requires a concerted effort and collaboration between governments, legislators, regulatory agencies, technology companies, digital platforms, civil society organisations, academic institutions and international organisations. Public-private partnerships and international harmonisation of regulations are consistently underscored as key remedial approaches to addressing the transnational character of deepfake-related cyber harm.
10. Social protection represents the ultimate governance objective	The review states that the main aim of the regulation of deepfake technology is to enhance social protection, including privacy, democratic integrity, public trust, cybersecurity, digital rights and individual dignity. Legal regulation and ethical compliance should therefore be regarded as complementary governance

	mechanisms to minimise cyber harm and to promote trustworthy AI ecosystems.
--	---

Summary of the Narrative Review Findings

The narrative review demonstrates how deepfake technology has evolved from a technological feat to a complex governance challenge with significant societal, ethical and legal implications. In the literature reviewed, there is often agreement among scholars that current legal frameworks are inadequate to the task of dealing with the rapidly evolving capabilities of artificial intelligence. Different countries like the United States, China, India and the European Union have come up with different regulatory solutions, but they remain fragmented, inconsistent and largely reactive. Although traditional legal doctrines, such as those governing privacy, defamation, copyright, cybercrime and data protection, continue to provide significant legal safeguards, they often struggle to address challenges such as AI-driven deception, anonymous creators, transborder circulation and pervasive online dissemination. This has led to a general agreement that specific and flexible regulations are required to better regulate deepfake technology.

Another interesting finding is the increasing importance of ethical compliance in AI governance. The body's research consistently demonstrates that regulation alone is insufficient to adequately address cyber damages associated with deepfake technology. In addition to legal obligations, ethical principles such as accountability, transparency, fairness, explainability, oversight by humans, and informed consent are additional governance mechanisms that foster responsible AI research and deployment. The assessment also highlights technology safeguards that strengthen legal enforcement and improve content authenticity, including blockchain-based authentication, digital watermarking, provenance verification, and AI-powered detection systems. But as accountability, liability and victims' rights are still essentially legal issues, these technical solutions cannot substitute for broad legislative control.

The analysis ends with the need for a layered and collaborative approach between governments, legislators, technology developers, digital platforms, civil society organisations and international regulatory authorities to effectively control deepfake technology. In addition to upholding the law, the ultimate goal is to enhance social protection by the protection of digital rights, privacy, democratic integrity, cybersecurity and public trust. The results of the study are a good theoretical basis for the conceptual framework in this study. Legal regulation is the independent variable, ethical compliance is conceptualised as the mediating variable, and social protection is the dependent variable. The overall narrative review indicates that tighter legal regulation improves the ethical compliance of the relevant actors, which in turn helps to improve protection against cyber damage caused by deepfake technology.

Development of the Theoretical Framework

The theoretical framework of the study is AI Governance Theory. It provides an appropriate framework to explain how governance mechanisms can effectively govern novel artificial intelligence technologies such as deepfakes. The AI Governance Theory states that responsible AI requires a strong governance ecosystem that includes institutional accountability, ethical principles, legal regulation, technological safeguards, and stakeholder collaboration along with

technological innovation (Shakil & Mekuria, 2024; Kishwar et al., 2025). From this perspective, ethical compliance is an extension of the legal requirement to promote transparency, accountability, fairness, human rights protection and responsible AI development, while legal regulation is the formal institutional rules governing the production, distribution and use of AI-generated synthetic media (Khanal & Koirala, 2026; Fernández et al., 2026). This theory is particularly relevant to the present study as deepfake technology raises governance issues that go beyond traditional legal boundaries such as identity theft, privacy breaches, misinformation, copyright infringement, political manipulation and cyber harm (Kukreti et al., 2026; Roy et al., 2026). AI Governance Theory argues that sustainable regulation should not be limited to law but should also add legal and ethical governance systems. In this study, legal regulation is conceptualised as the independent variable, representing institutional enforcement mechanisms, regulations, and statutory provisions governing deepfake technology. Ethical compliance is conceptualised as a mediating variable that translates legal requirements into responsible organisational and technical behaviour through voluntary adoption of ethical principles. Social protection is the dependent variable, which reflects the ultimate governance goal of protecting privacy, individual dignity, democratic integrity, cybersecurity, digital rights and public trust from the cyber harms of deepfake technology.

The conceptualisation of the proposed framework, showing the link of social protection, ethical compliance and legal control, is based on the recurrent patterns found throughout the narrative review. The literature reviewed consistently shows that despite the adoption of a variety of regulatory responses by governments such as the Digital Services Act, the General Data Protection Regulation (GDPR), the European Union's Artificial Intelligence Act, state legislation in the United States, China's regulations on synthetic media, and India's Information Technology Act, these legal structures remain fragmented, jurisdiction-specific, and largely reactive to technological developments (Bieñ-Węgawska, 2025; Kadri & West, 2025; Kakkar & Nandrajog, 2026). Therefore, scholars are proposing that ethical compliance is essential for effective governance to complement legal enforcement by integrating human supervision, transparency, explainability, accountability, informed consent, and fairness throughout the AI lifecycle (Fernández et al., 2026; Khanal & Koirala, 2026). This study also finds that companies with higher ethical compliance are more likely to develop preventive measures against deepfake misuse, strengthen internal accountability, adopt strong risk assessment procedures, and implement responsible AI governance practices (Hanna et al., 2026; Kishwar et al., 2025). The results theoretically confirm the proposition that ethical compliance is the mediation process through which legal regulation improves the effectiveness of governance. Ultimately, stronger ethical governance provides greater social protection by reducing cyber harms such as identity theft, online sexual exploitation, financial fraud, electoral manipulation, misinformation, reputational harm, and breaches of privacy and intellectual property rights (Boparai et al., 2026; Khare & Raghuwanshi, 2025; Verma, 2024).

The proposed theoretical framework has significant practical implications for lawmakers, policymakers, regulatory bodies, tech companies, digital platforms and international organisations tasked with governing AI. From a regulatory perspective, the framework advocates for legislative reforms that provide institutional ethical standards, AI risk management frameworks, transparency requirements, platform accountability and technological verification mechanisms such as blockchain authentication, digital watermarking, AI detection systems and content provenance verification (Hanna et al., 2026; Kukreti et al., 2026). To address the transnational dimension of deepfake-related cyber harm,

the framework also stresses the importance of collaborative governance among governments, private technology companies, civil society organisations, academia, and international institutions (Perriello, 2026; Shakil & Mekuria, 2024). The framework builds on and extends prior research and its policy implications by synthesising diverging legal, ethical and governance points of view into a unified theoretical model that explains the mechanisms through which legal regulation exerts an indirect influence on social protection via ethical compliance. This paradigm reveals the complementary relationship of legal institutions and ethical governance in controlling cyber harm related to deepfake technology, rather than the previous research that mainly focuses on legal doctrines or comparative legislation in isolation. Thus, the paradigm offers a theoretical basis for future empirical research to explore the causal links between societal protection, ethical compliance and legal regulation in different legal systems and within the framework of AI governance.

The three constructs have unique but interconnected roles in the proposed governance framework. Legal regulation is the formal basis for governance, it defines what is allowed and what is forbidden and creates binding obligations and accountability. Ethical compliance puts these requirements into practice, prompting stakeholders to translate regulatory expectations into responsible behaviour and, where appropriate, to establish safeguards beyond the minimum legal requirements. Social protection is the intended outcome of governance and refers to the protection of individuals, fundamental rights, democratic institutions, cyber security and public trust against deepfake related cyber harms.

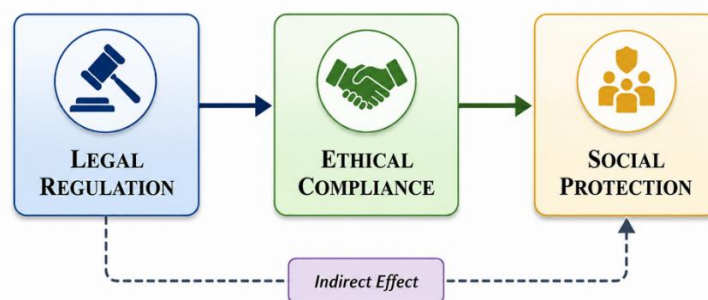


Figure 1: Theoretical Framework

Based on the narrative review and AI Governance Theory, the proposed relationship among the three constructs is shown in **Figure 1**. Legal regulation forms the formal institutional base, ethical compliance is the recommended operational mechanism for regulatory expectations, and social protection is the targeted governance outcome. Therefore, the framework proposes a pathway for addressing deepfake-related cyber harms by Legal Regulation → Ethical Compliance → Social Protection.

Proposition Development:

Legal Regulation Affects Social Protection

Legal regulation is the main institutional instrument that governments can use to reduce cyber damages caused by deepfake technology and to protect people, businesses, and society from AI-generated deception. Legal regulation refers to the formal standards, legislative

requirements, enforcement procedures, and institutional accountability that together govern the development, deployment, and misuse of artificial intelligence technology within the framework of AI Governance Theory. Literature has repeatedly shown that comprehensive legal regulation enhances privacy rights, protects personal data, combats misinformation, prevents identity theft, protects democratic processes, and addresses intellectual property infringement caused by deepfake technologies (Kishwar et al., 2025; Kukreti et al., 2026). Comparative regulatory developments further reinforce this link. For example, the United States has increasingly turned to state-level tort law, criminal penalties, and civil remedies to address deepfake-related harms, while the European Union has established a comprehensive regulatory framework with the Artificial Intelligence Act, the General Data Protection Regulation (GDPR), and the Digital Services Act. India continues to work toward bolstering its regulatory framework to address legislative gaps around deception that arises from AI, and China has also implemented regulations related to transparency and platform accountability (Bieč-Węęska, 2025; Kadri & West, 2025; Kakkar & Nandrajog, 2025; Perriello, 2026). Together, these legal developments show how stronger regulations strengthen institutional capacity to avoid cyber harm and better protect fundamental rights in the digital world.

Successful legal regulation therefore not only provides legal penalties but also ensures broader social protection, through the development of governance frameworks that stimulate ethical AI practices, enhance public trust in digital ecosystems and reduce societal exposure to misleading media. The narrative review finds that jurisdictions with more precise regulatory obligations, transparency requirements, and enforcement mechanisms are better equipped to combat cyberthreats related to deepfake technology (e.g., online harassment, election interference, financial fraud, non-consensual intimate imagery, and misuse of digital identities) (Boparai et al., 2026; Khanal & Koirala, 2026; Roy et al., 2026). AI Governance Theory also claims that regulatory certainty enables coordinated governance between governments, tech companies, digital platforms, and civil society organisations, thus raising institutional accountability and fostering a safer and more reliable digital space (Shakil & Mekuria, 2024). The law's regulation may not be able to completely eliminate cyber damages, but it does provide the legal framework that larger governance systems need to operate to improve social safety. Therefore, in terms of deepfake technology, the present study finds that more robust legal regulation is expected to have a positive effect on a higher degree of social protection.

Proposition 1 (P1): Legal regulation has a positive and significant effect on social protection in mitigating cyber harms associated with deepfake technology.

Legal Regulation Affects Ethical Compliance

Legal regulation makes a great contribution to the development of ethical compliance establishing formal norms, statutory requirements and accountability mechanisms that regulate the development and application of artificial intelligence technology. AI Governance Theory states that the legal structures not only define the appropriate behaviour, but also create institutional incentives for businesses, tech companies and online platforms to adopt moral behaviour beyond legal compliance. The European Union's Artificial Intelligence Act (AI Act), the General Data Protection Regulation (GDPR), the Digital Services Act and new national laws are already regulating deepfake technology, requiring more accountability, transparency, disclosure of content produced by AI and protection of fundamental rights. This encourages organisations to incorporate ethical principles in the AI governance (Bieč-Węęska, 2025; Kishwar et al., 2025; Perriello, 2026). 2. Given this rising anticipation for legal compliance to

be supported by responsible AI practices, institutional accountability and ethical decision-making, jurisdictions including the United States, China, and India have therefore enhanced or implemented legal measures tackling deepfake-related harms (Kakkar & Nandrajog, 2025; Kadri & West, 2025; Kukreti et al., 2026). Legal regulation is therefore a governance tool that fosters moral behaviour over the entire AI life cycle and a strong enforcement mechanism.

The literature published to date supports the view that stronger legal regulations encourage organisational cultures that value openness, justice, explainability, oversight by humans, informed consent and respect for human rights and privacy. As the law cannot foresee every novel technical risk nor regulate all forms of AI misuse, ethical compliance is more significant in the deepfake technology governance. Instead, legal structures can enable ethical-by-design approaches, AI risk assessments, better internal governance, and accountability mechanisms that mitigate cyber harm before the necessity for legal intervention arises (Fernández et al., 2026; Hanna et al., 2026; Khanal & Koirala, 2026). Academics further argue that legal certainty incentivises technology developers and digital platforms to embed ethical safeguards in the development, implementation, and oversight of artificial intelligence systems, which encourages responsible innovation and public trust in digital technologies (Roy et al., 2026; Shakil & Mekuria, 2024). Therefore, as predicted by the AI Governance Theory and the findings of the narrative review, it is expected that deeper legal regulation will positively impact the ethical compliance of stakeholders in the development and governance of deepfake technologies.

Proposition 2 (P2): Legal regulation has a positive and significant effect on ethical compliance in the governance of deepfake technology.

Ethical Compliance Affects Social Protection

Ethical compliance is an important governance tool that improves societal protection by encouraging the proper design, development, implementation and use of deepfake technologies. Ethical compliance encourages organisations, technology developers, digital platforms and AI practitioners to voluntarily adopt higher standards of responsibility than those that are statutorily required. Legal regulation provides mandated regulations and enforcement procedures. The AI Governance Theory emphasises the need for ethical principles like transparency, accountability, fairness, explainability, oversight by humans, respect for human rights and informed consent to guarantee that artificial intelligence serves societal interests while mitigating technological risks (Shakil & Mekuria, 2024). The application of deepfake technology in an ethical manner contributes to the well-being of society by reducing the likelihood of identity theft, online harassment, privacy violations, disinformation, electoral interference and the creation of non-consensual personal content. Scholars have argued that by embedding ethical-by-design principles throughout the AI lifecycle organisations can proactively identify risks, improve internal governance and protect people from new forms of cyber-harm before legal action is required (Fernández et al., 2026; Khanal & Koirala, 2026; Kishwar et al., 2025).

The study also indicates that ethical compliance for social protection is enhanced by promoting responsible innovation by stakeholders of the digital ecosystem and building public trust in artificial intelligence systems. Organisations that adopt ethical governance practices are more likely to adopt strong AI risk assessments, open content disclosure, bias mitigation techniques, privacy-preserving technologies and efficient monitoring systems that together mitigate the

societal risks of deepfake technology (Hanna et al., 2026; Roy et al., 2026). Ethical governance also encourages collaboration between governments, technology companies, civil society groups and regulators to create common standards for safeguarding cybersecurity, democratic integrity and digital rights (Kukreti et al., 2026; Perriello, 2026). Ethical compliance is an organisational responsibility and an important governance mechanism that contributes directly to greater social protection by improving personal safety, maintaining public trust and enhancing societal resilience to cyber harms arising from deepfake technology, the narrative review said. This study finds that better ethical compliance has a positive impact on social protection which is in line with AI Governance Theory as well as the findings of the narrative review.

Proposition 3 (P3): Ethical compliance has a positive and significant effect on social protection in mitigating cyber harms associated with deepfake technology.

The Mediating Role of Ethical Compliance in the Relationship Between Legal Regulation and Social Protection

Legislation alone cannot effectively regulate the emerging technology of artificial intelligence, according to AI Governance Theory. Rather, legal regulation provides the institutional framework that incentivises businesses, tech firms, digital platforms, and regulators to adopt moral standards that inform the responsible development and use of AI. Deepfake technology has been legislatively obligated to provide transparency, accountability, privacy protection, disclosure requirements, and platform duty. However, the effectiveness of such legal procedures depends on how far players internalise and implement moral principles such as justice, explainability, oversight by humans, informed consent and respect for fundamental rights (Khanal & Koirala, 2026; Kishwar et al., 2025). Research already indicates that ethical compliance operationalises legal requirements by incentivising organisations to go beyond minimum statutory duties and proactively manage AI-related risks before cyber damages take place (Fernández et al., 2026; Shakil & Mekuria, 2024). Hence, legal regulation increases the effectiveness of governance by incentivising moral behaviour that encourages responsible AI practices throughout the entire lifecycle of deepfake technologies.

The narrative evaluation also demonstrates that ethical compliance is an important process through which legal regulation produces meaningful social protection. Although the legal structures grant legislative powers to regulate the use of deepfake technology, legislation cannot foresee all types of technological developments and fully eliminate all types of cyber harms. Ethical compliance helps promote legal regulation and reduce the risk of malicious deepfakes (Hanna et al., 2026; Kukreti et al., 2026; Roy et al., 2026) by encouraging organisational accountability, transparent AI governance, responsible innovation, and ongoing risk management. In addition, companies embracing ethical governance in AI development are better positioned to implement preventative measures, transparent content authentication systems, and accountable decision-making processes that foster public confidence and enhance society's resilience to cyberattacks (Perriello, 2026). Therefore, this study posits that ethical compliance mediates the relationship between legal regulation and social protection by enhancing the effectiveness of legal governance to prevent cyber harms from deepfake technology in line with AI Governance Theory and the results of the narrative review.

Proposition 4 (P4): Ethical compliance positively mediates the relationship between legal regulation and social protection in mitigating cyber harms associated with deepfake technology.

Conclusion

To mitigate the cyber damage of deepfake technology, this study proposes a conceptual framework delineating the connection between legal regulation, ethical compliance, and social protection. The narrative assessment concludes that although many jurisdictions have passed legislation to regulate deepfake technology, existing regulatory structures are fragmented, reactive and insufficient to address the rapidly evolving issues presented by artificial intelligence. The results also show the need for ethical compliance, to supplement legal procedures in encouraging openness, accountability, fairness and responsible AI practices. Statutory regulation on its own cannot deliver effective governance. By theorising ethical compliance as the conceptualised mediating mechanism through which legal regulation improves social protection, the proposed framework advances AI Governance Theory and extends existing scholarship beyond isolated legal or ethical analyses toward an integrated governance perspective. In practical terms, the framework underscores the necessity of integrating legal reforms with ethical governance, technological safeguards and collaborative stakeholder engagement to bolster societal resilience against deepfake-related cyber harms. This information will be useful to legislators, regulatory bodies, technology developers, digital platforms and policy makers. However, there are several drawbacks to this study. The suggested associations are conceptual and have not been empirically tested, as this is a conceptual study using a narrative evaluation. The review also does not consider stakeholder perspectives or jurisdiction-specific implementation but is largely based on published literature already available. Therefore, the proposed paradigm will be empirically tested in different legal and regulatory contexts by employing quantitative, qualitative or mixed-method techniques in future studies. Further comparative cross-country studies, longitudinal investigations and research that incorporates additional governance variables, such as technological capability, institutional trust, regulatory enforcement, public awareness or organisational AI governance practices would further enhance the understanding of how integrated legal and ethical mechanisms can effectively protect society from the evolving cyber harms associated with deepfake technology.

-
- Acknowledgements:** The authors would like to express their sincere gratitude to the Kedah State Research Committee, UiTM Cawangan Kedah, for providing the necessary resources and support throughout this research. Special appreciation is extended to colleagues and peers in the Faculty of Law, UiTM Cawangan Kedah, who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.
- Funding Statement:** This research received financial support from the Kedah State Research Committee, UiTM Cawangan Kedah, through the *Tabung Penyelidikan AM*. The funding body had no role in the design of the study, data collection, analysis, interpretation of results, or the decision to publish this manuscript.
- 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 did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.
- Author Contribution Statement:** All authors contributed significantly to the development of this manuscript. Mohd Zulhelmey Abdullah was responsible for the conceptualisation, methodology, and overall supervision of the study. Siti Khadijah Abdullah Sanek and Irma Kamarudin handled data collection, analysis, and interpretation of results. Mohd Zulhelmey Abdullah, Nur Irinah Mohamad Sirat and Nurul Mazrah Manshor contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.
-

References

- Bień-Węglowska, I. (2025). Deepfakes in the light of the Artificial Intelligence Act. *Prawo i Więź*, 58(5), 152–169. <https://doi.org/10.36128/4dr67e80>
- Boparai, H., Kaur, R., Singh, G., & Gill, S. (2026). Privacy of minors in the deepfake era: A comparative study of India, the U.S. and China. In *Lecture Notes in Networks and Systems* (Vol. 1875, pp. 299–310). Springer. https://doi.org/10.1007/978-3-032-19684-2_29
- Chesney, B., & Citron, D. (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>
- de Ruiter, A. (2021). The distinct wrong of deepfakes. *Philosophy & Technology*, 34(4), 1311–1332. <https://doi.org/10.1007/s13347-021-00459-2>
- Fernández, Á. F., Rincón, I. M. B., & Aguirre, B. M. (2026). Ethics, personal image, and disinformation in the era of deepfakes. *VISUAL Review: International Visual Culture Review*, 18(2), 31–46. <https://doi.org/10.62161/revvisual.v18.5930>
- Hanna, E., Zahr, E. A., Samrouth, K., & Bakir, N. (2026). Technical framework for combating deepfake identity fraud in e-government services. In *Proceedings of the International Symposium on Digital Forensics and Security (ISDFS)*. <https://doi.org/10.1109/ISDFS69419.2026.11458925>
- Kadri, T. E., & West, S. R. (2025). Deepfake torts: Emerging tort frameworks in U.S. deepfake regulation. *Journal of Tort Law*, 18(2), 515–552. <https://doi.org/10.1515/jtl-2025-0032>
- Kakkar, L., & Nandrajog, A. B. (2025). Managing legal challenges in the current digital era: The deepfake dilemma in an Indian context. In *Deepfake Technology Dilemmas: Mastering Managerial Navigation* (pp. 129–148).
- Khanal, K., & Koirala, A. (2026). Deepfakes: Ethical and legal implications across business, politics, and society. In *Reshaping Journalism and Communications With AI* (pp. 189–208). IGI Global. <https://doi.org/10.4018/979-8-3373-2960-4.ch009>
- Khare, P., & Raghuwanshi, V. (2025). A complex intersection of deepfakes and copyright infringement. In *Legal and Economic Perspectives on the Nexus of AI and Copyright* (pp. 155–180). IGI Global. <https://doi.org/10.4018/979-8-3693-8704-7.ch008>
- 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>
- Kim, K. (2025). Deepfakes: Challenges to intellectual property rights in South Korea. *GRUR International*, 74(6), 532–542. <https://doi.org/10.1093/grurint/ikaf044>
- Kishwar, S. D., Tripathi, A., Khatoon, S., Poddar, D., & Khurana, B. (2025). Regulating deep fakes and synthetic media: Privacy, policy and global regulatory challenges. *Journal of Data Protection and Privacy*, 8(1), 78–96. <https://doi.org/10.69554/HBGG8150>
- Kukreti, A., Kumar, V., & Raj, A. (2026). The impact of deepfake technology on legal systems: A global perspective. *ShodhKosh: Journal of Visual and Performing Arts*, 7(1s), 530–544. <https://doi.org/10.29121/shodhkosh.v7.i1s.2026.7068>
- Okolie, C. (2023). Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns. *Journal of International Women's Studies*, 25(2), Article 11.
- Perriello, L. E. (2026). Blurred realities: Legal strategies for the deepfake era. *Maastricht Journal of European and Comparative Law*. Advance online publication. <https://doi.org/10.1177/1023263X261433380>
- Roy, A., Chattopadhyay, S., & Chakrabarty, S. P. (2026). Deepfakes: Navigating ethical concerns and legal frameworks. In *Lecture Notes in Networks and Systems* (Vol. 1513, pp. 337–355). Springer. https://doi.org/10.1007/978-981-96-8632-2_19

- Shakil, M., & Mekuria, F. (2024). Balancing the risks and rewards of deepfake and synthetic media technology: A regulatory framework for emerging economies. In *2024 International Conference on Information and Communication Technology for Development for Africa (ICT4DA)* (pp. 114–119). IEEE. <https://doi.org/10.1109/ICT4DA62874.2024.10777194>
- Singh, J., Das, R., Pradhan, S., Ojha, A., Mohapatra, H., & Mishra, S. R. (2025). Deepfake technology in India: Challenges, misuse trends, and policy recommendations. In *2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET)*. IEEE. <https://doi.org/10.1109/GIET65294.2025.11234747>
- Soneca, V. (2025). Risks and challenges of deepfakes in national and European parliament elections. In *Combating Misinformation and Global Nation's False Narratives Through Education* (pp. 149–172). IGI Global. <https://doi.org/10.4018/979-8-3693-9601-8.ch006>
- 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>
- Verma, K. (2024). Digital deception: The impact of deepfakes on privacy rights. *Lex Scientia Law Review*, 8(2), 859–896. <https://doi.org/10.15294/lslr.v8i2.13749>
- Vinogradov, V. A., & Kuznetsova, D. V. (2024). Foreign experience in legal regulating deepfake technology. *Pravo – Zhurnal Vysshey Shkoly Ekonomiki*, 17(2), 215–240. <https://doi.org/10.17323/2072-8166.2024.2.215.240>
- 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>