



Research Article

ARTIFICIAL INTELLIGENCE–GENERATED DEEPPAKES IN HIGHER EDUCATION: LEGAL RISKS, GOVERNANCE CHALLENGES, AND POLICY REFORM STRATEGIES

Author: Aaryan Sharma^{1*}, Bharat Chouhan² 

¹ Shri Jawaharlal Nehru Law College, Mandsaur (M.P.), 458002

² Acharya Rajendra Suri Shiksha Mahavidhyalaya (ARSSM) College of Pharmacy, Mandsaur (M.P.), 458002

KEYWORDS:

Deepfake Technology;
Artificial Intelligence; Higher
Education; Cyber Law;
Academic Integrity

ARTICLE HISTORY

Received Date: 05/04/2026

Revised Date: 08/04/2026

Accepted Date: 24/05/2026

Published Date: 08/06/2026

DOI: 10.69557/2czdkk06

CORRESPONDING AUTHOR

Aaryan Sharma

a9179899985@gmail.com

ABSTRACT

Deepfake technology, powered by artificial intelligence (AI) and deep learning algorithms, has rapidly evolved into a powerful tool capable of generating highly realistic synthetic audio, video, and image content. While the technology offers several legitimate applications in education, entertainment, and digital communication, its misuse has emerged as a significant concern for higher education institutions. Universities increasingly face challenges related to academic dishonesty, identity impersonation, misinformation, cyberbullying, reputational damage, and violations of privacy. Existing legal frameworks governing information technology, intellectual property, data protection, and cybercrime often fail to adequately address the unique characteristics of AI-generated deepfakes, thereby creating substantial policy gaps. The present study examined the legal implications of deepfake technology in higher education through a qualitative doctrinal research approach. Secondary data were collected from statutory provisions, judicial decisions, policy documents, international guidelines, and scholarly literature. The collected information was systematically categorized into legal, ethical, technological, and institutional dimensions to identify existing regulatory shortcomings and future policy requirements. The findings highlighted the urgent need for comprehensive legislation, institutional governance frameworks, AI literacy programs, digital authentication mechanisms, and interdisciplinary collaboration among policymakers, educational institutions, and technology developers. The study concluded that proactive legal reforms and preventive institutional strategies are essential to safeguard academic integrity, protect stakeholders' rights, and promote the responsible use of artificial intelligence within higher education.

INTRODUCTION

Artificial intelligence (AI) has transformed digital communication through the development of deep learning models capable of generating highly realistic synthetic media, commonly known as deepfakes. These AI-generated images, audio recordings, and videos have created unprecedented opportunities for innovation while simultaneously raising serious legal and ethical concerns within educational environments ^[1]. Higher education institutions increasingly rely on digital learning platforms, virtual classrooms, and online assessments, making them particularly vulnerable to the misuse of deepfake technologies for identity fraud, academic misconduct, misinformation, and reputational harm ^[2].

Deepfake-generated content has complicated traditional concepts of authenticity and evidentiary reliability, thereby challenging existing legal principles governing digital evidence and cybercrime investigations ^[3]. The rapid advancement of generative AI has also intensified concerns regarding privacy violations, unauthorized use of biometric information, copyright infringement, and data protection obligations in educational settings ^[4]. International organizations have emphasized the importance of developing trustworthy AI governance frameworks to ensure responsible technological innovation while protecting fundamental human rights ^[5].

Despite growing awareness of AI-related risks, many national legal systems continue to rely on fragmented legislation that was enacted before the emergence of sophisticated generative AI technologies ^[6]. Existing regulations frequently fail to provide explicit legal definitions, liability standards, or institutional responsibilities concerning deepfake misuse in universities ^[7]. Furthermore, policymakers have recognized that effective governance requires collaboration among governments, educational institutions, technology companies, and civil society organizations ^[8]. Scholars have also highlighted the necessity of integrating digital literacy, ethical AI education, cybersecurity awareness, institutional compliance mechanisms, and risk management strategies to reduce the societal impact of synthetic media in higher education ^[9–10]. Therefore, evaluating current legal frameworks and identifying future policy directions have become essential for maintaining academic integrity and protecting educational stakeholders.

RESEARCH METHODOLOGY

The present study was conducted using a qualitative doctrinal legal research design to examine the legal implications of deepfake technology in higher education and to identify existing policy gaps together with future regulatory directions. The research focused on evaluating existing legal frameworks, institutional policies, scholarly literature, judicial interpretations, and international guidelines governing artificial intelligence and synthetic media.

Research Design

A qualitative doctrinal methodology was adopted because the study primarily examined legal provisions, policy documents, and published academic evidence rather than collecting primary responses from human participants. The doctrinal approach enabled systematic interpretation of statutory provisions, regulatory frameworks, judicial precedents, and international recommendations relevant to deep-fake technology in educational institutions.

Sources of Data

Only secondary data were utilized during the investigation. A total of **150 documentary sources** were initially identified from internationally recognized databases and official publications.

The literature search was conducted using:

- Scopus
- Web of Science
- Google Scholar
- SpringerLink
- ScienceDirect
- IEEE Xplore
- SSRN
- HeinOnline
- Government legal portals
- UNESCO publications
- OECD reports
- European Union AI policy documents

The search was performed using combinations of the following keywords:

- "Deepfake Technology"
- "Artificial Intelligence"
- "Higher Education"
- "Cyber Law"
- "Digital Evidence"
- "Privacy Law"
- "Academic Integrity"
- "AI Governance"
- "Policy Framework"
- "Synthetic Media"

The literature covered publications released between **2019 and 2026**.

Table 1. Literature Search Strategy

Parameter	Description
Study Design	Qualitative doctrinal research
Nature of Data	Secondary data
Publication Period	2019–2026
Initial Documents Retrieved	150
Final Documents Reviewed	95
Databases Used	Scopus, Web of Science, Google Scholar, IEEE Xplore, SpringerLink, SSRN, HeinOnline, ScienceDirect
Language	English

Inclusion Criteria

The documents were included if they:

- discussed deepfake technology;
- examined legal, ethical, or policy implications of artificial intelligence;
- focused on higher education or educational governance;

- were published in peer-reviewed journals, official reports, statutes, policy documents, or judicial decisions;
- were written in English.

Exclusion Criteria

Documents were excluded when they:

- focused exclusively on technical algorithm development without legal discussion;
- consisted of conference abstracts lacking full text;
- were duplicate publications;
- were opinion articles without supporting legal or academic evidence;
- were unrelated to education or digital governance.

Following screening, **95 documents** satisfied the eligibility criteria and were included for detailed review.

Data Collection Procedure

The selected publications were downloaded in PDF format and organized using reference management software. Each document was assigned an identification code to facilitate systematic review. Relevant information relating to legal provisions, judicial observations, institutional governance, privacy regulations, intellectual property issues, academic misconduct, cybersecurity concerns, and policy recommendations was extracted using a structured data extraction sheet.

The extracted information was subsequently categorized into thematic domains to enable comparative legal interpretation.

Table 2. Data Extraction Categories

Category	Information Collected
Legal Framework	Statutes, regulations, judicial decisions
Privacy Issues	Personal data, biometric information, consent
Academic Integrity	Examination fraud, plagiarism, identity impersonation
Intellectual Property	Copyright ownership and infringement
Institutional Governance	University regulations and compliance mechanisms
Policy Recommendations	Legislative reforms and governance strategies

Document Analysis

The selected documents were analyzed using a structured thematic content-analysis approach informed by the study objectives and the legal issues identified during the literature review. The analysis was conducted in four sequential stages: familiarization, coding, categorization, and theme development.

First, all 95 eligible documents were read in full and relevant passages were extracted into a structured data-extraction matrix. The matrix recorded the document type, year of publication, jurisdiction or institutional context, legal issue addressed, applicable legal instrument, higher-education relevance, and policy recommendations.

Second, an initial coding framework was developed deductively from the research objectives and literature. The preliminary codes included academic integrity, privacy and data protection, identity impersonation, cybercrime and digital fraud, intellectual property, digital evidence, institutional governance, regulatory gaps, AI literacy, detection and authentication, and policy reform. Additional sub-codes were created when recurring concepts emerged during document review.

Third, conceptually similar codes were grouped into broader analytical categories. For example,

examination fraud, fabricated academic submissions, student impersonation, and falsified audiovisual evidence were grouped under the broader category of academic integrity. Similarly, unauthorized use of facial images, voice recordings, biometric identifiers, and personal data were grouped under privacy and data protection.

Fourth, the coded categories were reviewed against the original documents to identify recurring patterns, relationships, and differences across jurisdictions and institutional contexts. The final thematic structure comprised six principal domains: (i) academic integrity, (ii) privacy and data protection, (iii) identity impersonation and cybercrime, (iv) intellectual property and digital evidence, (v) institutional governance, and (vi) regulatory and policy gaps.

The analysis was primarily deductive because the principal legal domains were established from the research questions and existing legal literature. However, an inductive element was retained to allow additional issues to emerge from the reviewed documents. Themes were therefore considered sufficiently established when they recurred across multiple eligible documents and were directly relevant to the research objectives.

Legal Framework Assessment

To improve transparency, each eligible document was assigned a unique identification code (D01–D95). A document-level coding matrix was used to record whether each predefined theme was present, absent, or insufficiently described. A theme was counted as present when the document contained substantive discussion, evidence, legal analysis, or a policy recommendation relating to that theme. Mere incidental mention was not counted.

The frequencies presented in Tables 3, 4, and 6 therefore represent the number of reviewed documents in which a particular category or recommendation was identified. Percentages were calculated using the total number of eligible documents ($n = 95$) as the denominator:

Percentage (%) = $(\text{Number of documents coded for the category} / 95) \times 100$

Because a single document could address more than one legal issue or policy recommendation, the frequencies in Tables 4 and 6 are not mutually exclusive and therefore do not sum to 95.

For Table 3, each document was assigned to one primary publication type based on the nature of the source, making the categories mutually exclusive and allowing the total to equal 95.

The quantitative presentation is therefore descriptive rather than inferential. No statistical significance testing was undertaken because the study was based on documentary legal analysis rather than a probability sample of human participants.

Ethical Considerations

The quality and evidentiary relevance of the included material were assessed according to document type. Peer-reviewed articles were assessed for methodological clarity, relevance to the research question, transparency of evidence, and scholarly credibility. Government legislation, judicial decisions, and official regulatory documents were assessed primarily according to legal authority, jurisdictional relevance, authenticity, and direct applicability to the research question. International policy documents were assessed according to institutional authority, relevance, and policy specificity.

Documents that lacked sufficient substantive evidence, were purely opinion-based, or did not permit meaningful legal or policy analysis were excluded during screening. Because the study employed a doctrinal rather than systematic quantitative evidence-synthesis design, no numerical risk-of-bias score was assigned.

Study Limitations

The literature-selection process consisted of identification, duplicate removal, title and abstract screening, full-text eligibility assessment, and final inclusion. The initial search identified 150 records. Duplicate records were removed before title and abstract screening. The remaining records were screened against

the predefined inclusion and exclusion criteria. Full texts were subsequently assessed for legal, policy, or higher-education relevance, resulting in 95 documents being included in the final qualitative analysis. The review and coding process followed a structured workflow in which the eligibility criteria and coding categories were established before detailed extraction. The authors independently checked the eligibility and coding decisions for consistency, and disagreements were resolved through discussion and reference to the predefined criteria. The final dataset was then used for thematic and descriptive analysis.

RESULTS AND DISCUSSION

A total of **150 documents** were initially retrieved from eight electronic databases and official legal repositories. After removing duplicate records (n = 22) and screening titles and abstracts, **128 publications** remained for further evaluation. An additional **33 documents** were excluded because they focused solely on technical aspects of deepfake generation or lacked relevance to higher education law. Finally, **95 documents** satisfied all inclusion criteria and were included in the qualitative legal analysis. The review demonstrated that the increasing accessibility of generative artificial intelligence had significantly expanded the potential misuse of deepfake technology within higher education institutions. The identified legal issues were categorized into six major domains: academic integrity, privacy and data protection, intellectual property, cybercrime and identity fraud, institutional governance, and regulatory policy gaps.

1 Distribution of Reviewed Literature

The reviewed documents represented a diverse range of publication types, indicating growing multidisciplinary interest in regulating artificial intelligence within education.

Table 3. Distribution of Selected Documents by Publication Type

Publication Type	Number (n=95)	Percentage (%)
Research Articles	48	50.5
Review Articles	18	18.9
Government Reports	9	9.5
International Policy Documents	8	8.4
Legal Acts and Regulations	6	6.3
Judicial Decisions	3	3.2
Institutional Guidelines	3	3.2
Total	95	100.0

Research articles constituted more than half of the reviewed literature (50.5%), followed by review papers (18.9%). Official government reports, international policy documents, and legal regulations together accounted for nearly one-fourth of the evidence base, indicating increasing governmental attention toward AI governance.

Legal Issues Identified in Higher Education

The thematic analysis identified multiple legal concerns associated with deepfake technology. Academic integrity emerged as the most frequently discussed issue, particularly regarding examination malpractice, student impersonation, fabricated academic evidence, and falsified audiovisual submissions. Privacy violations represented another major concern. Several publications reported that deepfake software frequently relied upon unauthorized collection of facial images, voice recordings, and biometric

identifiers obtained from publicly accessible digital platforms without informed consent. Such practices potentially violated existing privacy and data protection legislation.

Intellectual property concerns were also repeatedly identified. Unauthorized reproduction of lecturers' instructional videos, AI-generated modifications of educational materials, and manipulation of copyrighted digital content created uncertainty regarding ownership rights and legal liability.

Cybercrime-related issues included identity theft, phishing attacks, reputational damage, digital blackmail, misinformation campaigns, and fraudulent online communications targeting students, faculty members, and institutional administrators.

Institutional governance challenges primarily involved the absence of dedicated university policies regulating artificial intelligence applications, insufficient verification systems for digital examinations, and limited awareness among academic communities regarding synthetic media.

Frequency of Major Legal Concerns

Table 4. Major Legal Issues Identified in the Reviewed Literature

Legal Issue	Frequency (n=95)	Percentage (%)
Academic Integrity Violations	82	86.3
Privacy and Data Protection	78	82.1
Identity Impersonation	74	77.9
Cybercrime and Digital Fraud	69	72.6
Intellectual Property Issues	63	66.3
Institutional Policy Deficiencies	60	63.2
Digital Evidence Challenges	55	57.9

Academic integrity violations were reported in 86.3% of the reviewed documents, making them the most prominent concern. Privacy-related issues (82.1%) and identity impersonation (77.9%) closely followed. More than two-thirds of the literature discussed cybercrime and copyright-related implications, reflecting the broad legal consequences of synthetic media within educational environments.

Assessment of Existing Legal Frameworks

The analysis revealed that although numerous countries possessed legislation governing cybercrime, privacy protection, electronic records, and copyright, only a limited number had enacted legislation specifically addressing deepfake technology.

Most existing legal systems regulated only the consequences of unlawful conduct rather than the creation, distribution, or educational misuse of AI-generated synthetic media. Consequently, universities often relied upon general information technology laws or institutional disciplinary regulations when addressing deepfake-related incidents.

International policy frameworks issued by UNESCO, the OECD, and the European Union emphasized ethical AI governance, transparency, accountability, and human rights protection. However, these documents functioned primarily as policy recommendations rather than legally enforceable instruments.

Institutional Preparedness

The reviewed evidence suggested that institutional preparedness remained relatively limited. Only a minority of higher education institutions had developed formal AI governance policies or digital authentication procedures capable of detecting manipulated audiovisual content.

Many universities continued to depend upon conventional plagiarism detection software, which demonstrated limited effectiveness in identifying AI-generated images, videos, or voice recordings. Furthermore, faculty training regarding deepfake identification remained insufficient in many institutions.

Table 5. Institutional Preparedness Measures Reported in the Reviewed Literature

Institutional Measure	Documents Reporting the Measure (n=95)	Percentage (%)
AI Ethics Policy	38	40.0
Digital Identity Verification	35	36.8
Faculty AI Training Programs	29	30.5
Deepfake Detection Software	24	25.3
Student AI Awareness Programs	32	33.7
Incident Reporting Mechanism	27	28.4

Note: Frequencies represent the number of reviewed documents that reported, recommended, evaluated, or discussed the corresponding institutional measure. Categories were not mutually exclusive. Percentages were calculated as the frequency divided by the 95 documents included in the final analysis.

The legal approaches examined in the reviewed literature demonstrate that jurisdictions have adopted substantially different strategies for addressing AI-generated synthetic media. These approaches can broadly be differentiated into risk-based regulation, conduct-specific regulation, and fragmented sectoral regulation.

The European Union provides the most structured risk-based approach through the EU Artificial Intelligence Act. Of particular relevance to higher education is Article 50, which establishes transparency obligations concerning certain AI-generated or manipulated content, including deepfakes. The European Commission's implementation guidance confirms that the transparency obligations under Article 50 apply from 2 August 2026 and require appropriate disclosure and marking of AI-generated or manipulated content.

This approach has significant implications for universities. Higher education institutions operating or collaborating within the EU regulatory environment may need to establish procedures for identifying AI-generated content, informing users when they interact with certain AI systems, documenting institutional use of AI tools, and incorporating transparency requirements into assessment and digital-media policies. The EU model therefore moves beyond the simple prohibition of harmful conduct and introduces preventive transparency and accountability mechanisms.

The United States demonstrates a comparatively more fragmented approach. Rather than relying exclusively on a single comprehensive federal framework for all forms of deepfake misuse, regulation has developed through a combination of sector-specific and state-level measures. The federal TAKE IT DOWN Act, enacted in May 2025, addresses the non-consensual online publication of intimate visual depictions, including computer-generated depictions, and establishes removal obligations for covered platforms. This conduct-specific approach provides important protection against a particularly harmful category of synthetic media but does not constitute a comprehensive higher-education governance framework.

India has also moved toward more explicit regulation of synthetically generated information. The Ministry of Electronics and Information Technology's 2026 update to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules introduced provisions concerning synthetically generated information, including requirements relating to labelling, visibility, and identification of synthetic content. These developments are particularly relevant to Indian universities because deepfake incidents may involve students, faculty, institutional communications, examinations, and online learning environments.

The comparison indicates that no single jurisdictional model completely resolves the higher-education problem. The EU approach offers stronger preventive transparency and risk governance; the United States illustrates the value of targeted protection against specific forms of harm; and India's developing framework demonstrates the importance of intermediary accountability and content identification. For universities, these approaches suggest that legal compliance should not be limited to responding after

harmful content has been disseminated. Institutional policies should incorporate preventive risk assessment, provenance and labelling mechanisms, incident response, privacy safeguards, procedural fairness, and user education.

Future Policy Directions

The documentary evidence consistently emphasized the necessity for comprehensive legislative reforms specifically addressing AI-generated synthetic media. The proposed policy directions included establishing statutory definitions of deepfakes, introducing criminal and civil liability provisions for malicious creation and dissemination, strengthening privacy protections for biometric information, clarifying copyright ownership of AI-generated educational content, and developing mandatory institutional AI governance policies.

The reviewed publications further recommended integrating digital literacy programs into university curricula to improve awareness among students and faculty regarding responsible AI use. Collaboration among governments, educational institutions, technology developers, and regulatory agencies was also identified as essential for developing standardized detection technologies and harmonized legal frameworks.

Table 6. Recommended Policy Priorities Identified in the Literature

Policy Recommendation	Frequency (n=95)
Comprehensive Deepfake Legislation	84
Institutional AI Governance Policies	80
Digital Literacy and AI Education	76
Privacy and Biometric Protection	74
AI Detection Technologies	69
International Regulatory Cooperation	66
Faculty Capacity Building	61

Based on the comparative analysis, this study proposes an Institutional Deepfake Governance Model consisting of six interconnected components: **Governance, Prevention, Authentication, Response,**

Rights Protection, and Review.

- 1. Governance:** Each university should establish an AI governance committee or designate an institutional AI compliance officer responsible for developing policies on synthetic media, monitoring regulatory developments, and coordinating legal, academic, technological, and ethical responses.
- 2. Prevention:** Institutions should adopt clear rules defining acceptable and prohibited uses of synthetic media. Academic regulations should distinguish legitimate educational applications from impersonation, fraudulent submissions, harassment, manipulation of institutional communications, and unauthorized use of personal likeness or voice.
- 3. Authentication:** Universities should implement proportionate verification mechanisms for high-risk activities, particularly online examinations, official announcements, identity-sensitive communications, and digitally submitted audiovisual evidence. Authentication should not depend exclusively on automated deepfake-detection software because detection systems may produce false positives and false negatives.
- 4. Response:** A documented incident-response mechanism should provide a confidential reporting channel, preliminary verification, preservation of relevant digital evidence, escalation to appropriate institutional authorities, and referral to law-enforcement or regulatory bodies where legally necessary.

5. Rights Protection: Institutional responses should incorporate privacy, data protection, freedom of expression, academic freedom, due process, and protection against wrongful disciplinary action. Students and staff accused of creating or distributing manipulated media should receive an opportunity to respond to allegations and challenge unreliable evidence.

6. Review and Capacity Building: Policies should be reviewed periodically because synthetic-media technologies and applicable legal requirements evolve rapidly. Universities should provide continuing AI-literacy and digital-authentication training to students, faculty, administrators, and technical staff.

Table 7. Proposed Institutional Legal Governance Framework for Deepfake Management in Higher Education

Governance Domain	Institutional Requirement	Responsible Authority	Key Compliance Mechanism
AI Governance	University-wide synthetic-media policy	AI Governance Committee	Annual policy review
Academic Integrity	Rules for AI-assisted and synthetic-media submissions	Academic Council/Examination Cell	Assessment verification
Identity Protection	Protection of faculty/student likeness and voice	Data Protection/IT Office	Consent and authentication
Privacy	Safeguards for biometric and personal data	Data Protection Officer/IT Office	Data minimization and access control
Content Transparency	Identification of AI-generated or manipulated content	IT/Communication Office	Labelling and provenance
Incident Response	Reporting and investigation procedure	Grievance/Compliance Committee	Documented incident-response protocol
Digital Evidence	Preservation and verification of disputed media	IT/Cybersecurity Unit	Chain-of-custody procedures
Capacity Building	AI literacy and deepfake awareness	Faculty Development/Student Affairs	Periodic training
Legal Escalation	Referral of serious cases to competent authorities	Legal/Compliance Office	Jurisdiction-specific legal review
Monitoring and Review	Periodic assessment of policy effectiveness	AI Governance Committee	Annual compliance audit

The proposed model converts broad legal principles into an institutional compliance structure. It therefore provides a practical bridge between external regulation and university-level governance. UNESCO's guidance similarly emphasizes the need for coherent policy frameworks, data protection, human-centred governance, and capacity building in educational contexts.

CONCLUSION

The present study examined the legal risks, governance challenges, and policy requirements associated with AI-generated deepfakes in higher education. The documentary analysis indicates that deepfake-

related risks extend across academic integrity, privacy and data protection, identity impersonation, cybercrime, intellectual property, digital evidence, and institutional accountability. Although existing legal systems provide mechanisms that may be applied to several forms of unlawful synthetic-media activity, regulatory protection remains uneven and institutional governance mechanisms are still developing.

The comparative analysis demonstrates that different jurisdictions provide complementary approaches rather than a single comprehensive solution. The European Union's risk-based and transparency-oriented framework provides a strong model for preventive governance, while the United States illustrates the importance of targeted legal remedies for specific forms of harmful synthetic media. India's evolving regulation of synthetically generated information further demonstrates the growing importance of content identification, intermediary responsibility, and technological safeguards.

On the basis of these findings, this study proposes an Institutional Deepfake Governance Model incorporating governance, prevention, authentication, incident response, rights protection, and continuous review. The model is intended to assist universities in translating general AI principles and external legal requirements into practical institutional compliance mechanisms.

Future research should move beyond doctrinal analysis by empirically examining the preparedness of higher education institutions, students, faculty members, and administrators. Comparative empirical studies could evaluate how universities in different jurisdictions implement deepfake policies and whether institutional governance mechanisms effectively reduce academic misconduct and privacy risks. Further research should also assess the accuracy, reliability, and fairness of automated deepfake-detection technologies, particularly in disciplinary and examination contexts where false accusations may have serious consequences. Longitudinal studies will be necessary to evaluate how university policies respond to rapidly changing generative-AI capabilities and emerging regulatory requirements. Finally, interdisciplinary research combining law, education, cybersecurity, computer science, and ethics could contribute to the development of evidence-based standards for authenticating digital academic evidence while preserving privacy, academic freedom, and procedural fairness.

Overall, effective deepfake governance in higher education requires a transition from reactive responses to proactive institutional risk management. Universities should therefore integrate legal compliance, technological safeguards, AI literacy, transparent procedures, and human oversight into a continuous governance framework capable of adapting to technological and regulatory change.

REFERENCES

1. Chesney, R.; Citron, D. K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *Calif. Law Rev.* **2019**, *107* (6), 1753–1820.
2. Westerlund, M. The Emergence of Deepfake Technology: A Review. *Technol. Innov. Manage. Rev.* **2019**, *9* (11), 39–52.
3. Roe J, Perkins M, Somoray K, Miller D, Furze L. To Deepfake or Not to Deepfake: Higher Education Stakeholders' Perceptions and Intentions towards Synthetic Media. 2025.
4. Almási Z, Bleher H, Bleher J, et al. AI Governance in Higher Education: A Course Design Exploring Regulatory, Ethical and Practical Considerations. 2025.
5. Gazis A, Chamalidou E, Ntaoulas N, Vavouras T. Synthetic Media in Multilingual MOOCs: Deepfake Tutors, Pedagogical Effects, and Ethical-Policy Challenges. 2026..
6. European Parliament. *Artificial Intelligence Act (AI Act)*; European Union: Brussels, Belgium, 2024.
7. OECD. *OECD Principles on Artificial Intelligence*; Organisation for Economic Co-operation and Development: Paris, France, 2019.
8. European Commission. *Ethics Guidelines for Trustworthy Artificial Intelligence*; High-Level Expert Group on AI; European Commission: Brussels, Belgium, 2019.

9. Dwivedi, Y. K.; Hughes, L.; Baabdullah, A. M.; et al. So What If ChatGPT Wrote It? Multidisciplinary Perspectives on Opportunities, Challenges, and Implications of Generative Conversational AI for Research, Practice, and Policy. *Int. J. Inf. Manage.* **2023**, *71*, 102642.
10. Kasneci, E.; Sessler, K.; Küchemann, S.; Bannert, M.; Dementieva, D.; Fischer, F.; et al. ChatGPT for Good? On Opportunities and Challenges of Large Language Models for Education. *Learn. Individ. Differ.* **2023**, *103*, 102274.

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AI	Artificial Intelligence
EU	European Union
GenAI	Generative Artificial Intelligence
HEI	Higher Education Institution
IT	Information Technology
OECD	Organisation for Economic Co-operation and Development
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
UNESCO	United Nations Educational, Scientific and Cultural Organization
SIG	Synthetically Generated Information
GDPR	General Data Protection Regulation
IP	Intellectual Property
U.S.	United States