

Deepfakes and Intellectual Property: Copyright licensing, personality rights, and civil/criminal liability for synthetic media generation

Dr. Bhavana C

Principal Harsha School of Law bhavanaballb@gmail.com

HOW TO CITE:

Bhavana C (2026). Deepfakes and Intellectual Property: Copyright licensing, personality rights, and civil/criminal liability for synthetic media generation International Journal of Special Education, 41(25s), 992-1007

ABSTRACT:

Background. Generative AI now makes realistic synthetic video, images and voices of real people cheap and widespread. Law must deter non-consensual deepfakes while allowing a lawful market in licensed digital replicas, but copyright, personality rights and criminal law each address only part of the problem.

Objective. To compare how legal systems allocate control over a person's likeness and voice, govern licensing, and distribute civil and criminal liability for synthetic media.

Methods. A doctrinal, functional comparative analysis of eight legal systems (the EU layer, Italy, the United Kingdom, the United States, China, South Korea, India and Bangladesh) as of 20 October 2026. Each system was scored on a nine-dimension Synthetic Media Legal Coverage Index (SMLCI, 0–18) grouped into three pillars: rights and licensing, transparency and platforms, and liability. Four IP-style likeness-right models (Denmark, Cyprus, the U.S. NO FAKES bill and Tennessee's ELVIS Act) were compared separately.

Results. SMLCI scores ranged from 6 (Bangladesh; 33.3%) to 15 (United States; 83.3%), with a mean of 9.9. The rights and licensing pillar reached only 32.8% of its maximum, against 75.0% for transparency and platforms and 70.8% for liability. Sexual-deepfake offences were the most widely covered dimension (87.5%), while copyright or IP vehicles for likeness (6.3%) and post-mortem control (25.0%) were the least. Rankings were robust to equal pillar weighting (Spearman $\rho = 0.99$).

Conclusion. Deepfake law has built sanctions and takedown duties faster than the property and licensing rules that define lawful use. Copyright is best used as an enforcement container for a dignity-based personality right, not as its foundation. A four-layer model (right, licence, transparency, liability) is proposed for jurisdictions such as Bangladesh.

Keywords: deepfakes; synthetic media; copyright; personality rights; right of publicity; digital replicas; AI regulation; comparative law

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Introduction

Synthetic media has moved from a research curiosity to a mass-market capability in under a decade. Generative adversarial networks (Goodfellow et al., 2014) and later diffusion and voice-cloning models now let any user produce realistic video, images and speech of a real person from a few seconds of source material (Mirsky & Lee, 2021; Tolosana et al., 2020). The word “deepfake” entered public use in 2017, and early

audits found that the overwhelming majority of deepfakes circulating online were non-consensual sexual content targeting women (Ajder et al., 2019).

The harms are now well documented. Deepfakes enable sexual abuse, fraud, reputational attack and political disinformation, and they erode trust even in authentic media (Chesney & Citron, 2019; Vaccari & Chadwick, 2020). At the same time, the same tools support legitimate creative and

commercial uses: dubbing, posthumous performances, licensed voice models and advertising (Kietzmann et al., 2020; Westerlund, 2019). Law must therefore do two things at once: stop non-consensual replication of identity, and enable a lawful market in consented digital replicas.

Existing legal tools fit this task poorly. Copyright protects original works, not a person's face or voice, and recent decisions confirm that machine output without human authorship is not protected (Thaler v. Perlmutter, 2025; U.S. Copyright Office, 2024). Personality and publicity rights protect identity, but they vary sharply between jurisdictions, are often limited to commercial use, and are absent in many common-law systems (Rothman, 2018). Criminal law has reacted unevenly, focusing first on sexual deepfakes and only later on fraud and impersonation (Delfino, 2019; Meskys et al., 2020).

Since 2024 the legislative picture has changed quickly. The EU Artificial Intelligence Act imposes disclosure duties for deepfakes; Denmark and Cyprus have created new IP-style rights over voice and appearance; the United States has enacted a federal criminal and takedown regime for intimate deepfakes while states expand publicity rights. Yet the scholarship remains largely single-jurisdiction and doctrinal. No study, to our knowledge, systematically codes how copyright licensing, personality rights and civil/criminal liability interact across both Global North and Global South jurisdictions, including the 2025–2026 reforms.

Research gap and novelty. This article fills that gap with a structured comparative analysis of eight legal systems (the EU layer, Italy, the United Kingdom, the United States, China, South Korea, India and Bangladesh), scored on a transparent nine-dimension Synthetic Media Legal Coverage Index (SMLCI), plus a focused comparison of four IP-style likeness-right models. To the best of our knowledge, it is the first study to place the 2025–2026 reforms in Europe, the United States and East and South Asia, together with the

Danish, Cypriot and proposed U.S. federal likeness rights, within one coded framework.

The study asks four research questions:

1. **RQ1.** How do jurisdictions allocate protection of a person's likeness and voice between copyright-type rights and personality rights?
2. **RQ2.** What rules govern licensing, transfer and post-mortem control of digital replicas?
3. **RQ3.** How are civil and criminal liabilities distributed among creators, deployers and platforms of synthetic media?
4. **RQ4.** What regulatory model best fits jurisdictions without a dedicated regime, with Bangladesh as a test case?

The article proceeds as follows. Section 2 reviews the literature and sets out the conceptual framework. Section 3 explains the doctrinal-comparative method and coding scheme. Section 4 reports the coded results, Section 5 discusses them, and Section 6 offers policy recommendations, limitations and conclusions.

2. Literature Review and Theoretical Framework

2.1 Synthetic media: capability and harm

Technical surveys describe deepfakes as outputs of generative models that swap, re-enact or fully synthesise faces and voices (Mirsky & Lee, 2021; Tolosana et al., 2020). Detection keeps improving, but the same surveys show that generation improves faster, so law cannot rely on technical detection alone. Scholars group the resulting harms into three clusters: harms to the depicted person (sexual abuse, reputational and economic injury), harms to audiences (fraud and deception) and harms to collective trust (disinformation and the “liar's dividend”) (Chesney & Citron, 2019; Paris & Donovan, 2019).

Sexual deepfakes dominate both the empirical record and the ethical literature. Ajder et al. (2019) found that non-consensual pornography made up the large majority of deepfake videos

online, almost entirely targeting women. Öhman (2020) argues that the wrong lies in the instrumentalisation of a person's identity even when no viewer is deceived, and Gosse and Burkell (2020) show that news coverage framed deepfakes around four problems, from ease of production and false beliefs to political manipulation and non-consensual sexual content, with uneven emphasis across them. This literature explains why criminal law moved first on intimate imagery (Delfino, 2019).

Audience-side evidence is more mixed. In an experiment, Vaccari and Chadwick (2020) found that synthetic political video did not always deceive viewers but significantly increased uncertainty, which in turn reduced trust in news. Business scholarship adds that the same technology creates value in marketing, entertainment and training, so regulation must separate consented from non-consented uses (Kietzmann et al., 2020; Westerlund, 2019).

2.2 Copyright: a poor fit for identity

Copyright protects original expression, defined in EU law as the author's own intellectual creation (Infopaq, 2009). A face or a voice is not a work, so copyright protects the photographs or recordings used as source material, not the person they depict (Meskys et al., 2020). Copyright therefore helps a photographer or a record label against a deepfake but rarely helps the person portrayed.

Copyright also struggles with the output side. U.S. courts and the U.S. Copyright Office hold that human authorship is required, so purely machine-generated material is not protected (Thaler v. Perlmutter, 2025; U.S. Copyright Office, 2024). Ginsburg and Budiardjo (2019) reach the same conclusion doctrinally, and Samuelson (2023) shows that the live disputes concern training data and output similarity rather than identity. The U.S. Copyright Office (2024) accordingly recommended a new federal digital-replica right outside copyright.

A minority view now treats IP-style rights as a practical enforcement vehicle. Denmark's bill and

Cyprus's 2026 law place a new likeness right inside copyright or neighbouring-rights legislation, mainly to reuse familiar notice-and-takedown and remedy machinery (Bill L 49, 2026; Law 29(I)/2026). Critics answer that copyright-style rights are assignable, while dignity-based personality rights are not, so commodifying identity may leave weaker parties exposed.

2.3 Personality and publicity rights

U.S. publicity law grew from *Haelan Laboratories v. Topps Chewing Gum* (1953) and was confirmed by the Supreme Court in *Zacchini v. Scripps-Howard Broadcasting* (1977). *Midler v. Ford Motor Co.* (1988) extended protection to imitation of a distinctive voice, a direct precursor of voice-cloning disputes. Rothman (2018) shows that the resulting state-by-state system is inconsistent, especially on assignability and post-mortem rights.

Civil-law systems protect the image as a personality right grounded in dignity. Italy's Civil Code (art. 10) and Copyright Law (arts. 96–97) require consent for exhibiting a person's portrait, and China's Civil Code (2020) expressly forbids forging a portrait by information technology (art. 1019) and extends the same protection to voice (art. 1023). Common-law India and the UK have no statutory right; Indian courts build personality rights from constitutional privacy and passing off (*Anil Kapoor v. Simply Life India*, 2023; Puttaswamy, 2017), while English courts rely on passing off (*Irvine v. Talksport*, 2002).

2.4 Liability for synthetic media

The liability literature asks three questions: who is liable (creator, commissioner, distributor, platform or tool provider), for what (creation, possession or distribution) and on what mental state. Chesney and Citron (2019) warned that civil suits alone would fail because creators are anonymous and often judgment-proof, which pushes regulation toward platforms. Delfino (2019) argued for federal criminalisation of pornographic deepfakes, a position later reflected in the TAKE IT DOWN Act (2025).

2.5 Gap in the literature

Three gaps follow. First, most legal studies analyse one jurisdiction or one regime (copyright *or* publicity *or* criminal law), not their interaction. Second, comparative work rarely includes South and East Asian systems, despite India's 2026 labelling rules, South Korea's 2024 criminal reforms and Bangladesh's 2026 Cyber Security Act. Third, there is no transparent, replicable metric for comparing how completely a legal system covers synthetic-media risks.

2.6 Conceptual framework

This study treats synthetic-media governance as three interacting pillars (Figure 1). **Pillar A, Rights and licensing**, decides who controls a likeness and how consent is given, transferred and inherited. **Pillar B, Transparency and platform governance**, imposes ex ante duties to label content and remove unlawful material. **Pillar C, Liability**, supplies ex post civil and criminal sanctions. The framework predicts that coverage in one pillar cannot compensate for gaps in another: a strong likeness right without platform duties is hard to enforce, and criminal law without a licensing regime chills lawful uses.

Figure 1. Deepfake governance rests on three interacting pillars

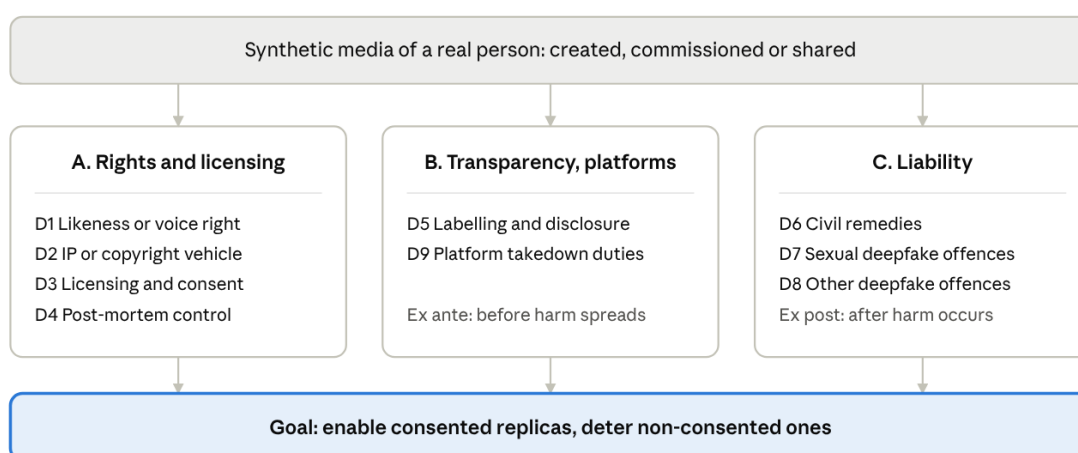


Figure 1. Conceptual framework of the study. Each pillar maps onto the coding dimensions used in Section 3; source: authors' framework.

3. Methodology

3.1 Research design

The study uses a qualitative doctrinal and comparative legal design. It follows the functional method of comparative law, which compares how different systems solve the same social problem rather than comparing legal labels (Zweigert & Kötz, 1998). To make the comparison transparent and replicable, the doctrinal analysis is converted into a structured ordinal coding scheme, an approach known as leximetric or numerical comparative law (Siems,

2005). No human participants were involved, so ethical approval was not required.

3.2 Sample selection

Eight legal systems were selected purposively for maximum variation on four criteria: legal family (civil law, common law, socialist civil law and mixed systems); legislative activity on synthetic media between 2023 and 2026; representation of the Global South; and availability of the primary text in English or a reliable translation. The EU is coded as a supranational layer that applies on top of national law in its member states.

Four IP-style likeness-right models are analysed separately in Section 4.4 rather than scored. Denmark's bill (L 49) and the U.S. NO FAKES Act of 2026 were still pending at the cut-off date, and a full English text of Cyprus's Law 29(I)/2026 was not available to the author; scoring them alongside enacted systems would mix law in force with proposals. Tennessee's ELVIS Act (2024) is included in that comparison as the leading enacted U.S. state model.

3.3 Data sources and cut-off

Primary sources were statutes, regulations, bills and judgments. Secondary sources were peer-reviewed legal and technical literature, official

reports (such as U.S. Copyright Office, 2024) and practitioner briefings used only to confirm dates of enactment and entry into force. The legal position is stated as of 20 October 2026.

3.4 Coding scheme

Each legal system was scored on nine dimensions grouped under the three pillars of Figure 1 (Table 1). Every dimension uses the same three-point ordinal scale: **0** = absent; **1** = partial, general or indirect coverage (for example, a general fraud offence or a judge-made right); **2** = explicit coverage of synthetic media or digital replicas in a binding instrument in force.

Table 1. Codebook of the Synthetic Media Legal Coverage Index (SMLCI)

Pillar	Dimension	Score 2 (explicit)	Score 1 (partial)
A. Rights and licensing	D1 Likeness or voice right	Statute expressly covers digital or synthetic replicas	General image, privacy or publicity right, or judge-made right
A. Rights and licensing	D2 IP or copyright vehicle	Likeness right housed in copyright or neighbouring-rights law and covering synthetic imitation	Portrait or performer rules inside copyright law, not specific to synthetic media
A. Rights and licensing	D3 Licensing and consent	Specific rules on consent or contracts for digital replicas	General data-protection or portrait-consent rules applied to likeness
A. Rights and licensing	D4 Post-mortem control	Statutory post-mortem right covering digital replicas	General post-mortem claims by relatives or estates
B. Transparency and platforms	D5 Labelling and disclosure	General mandatory labelling of synthetic content	Disclosure limited to one sector, such as elections
B. Transparency and platforms	D9 Platform takedown duties	Specific notice, removal deadline or proactive duty for synthetic or intimate content	General intermediary notice-and-action duties
C. Liability	D6 Civil remedies	Damages or injunctions expressly tied to synthetic likeness	General tort, defamation, privacy or passing-off remedies
C. Liability	D7 Sexual deepfake offences	Offence expressly covering synthetic sexual content	Only general obscenity, voyeurism or harassment offences
C. Liability	D8 Other deepfake offences	Offence expressly targeting non-sexual harmful synthetic media	Only general fraud, impersonation or defamation offences

Note. Score 0 = no relevant binding rule. A rule scores only if it was in force, or legally binding on the system as a supranational obligation, on 20 October 2026.

3.5 Index construction and robustness

The SMLCI is the unweighted sum of the nine scores, ranging from 0 to 18, and is also expressed as a percentage of the maximum. Pillar sub-indices are A (D1–D4, maximum 8), B (D5 and D9, maximum 4) and C (D6–D8, maximum 6). Because pillar A has more dimensions, the unweighted sum gives it more weight; a robustness index therefore weights the three pillars equally:

$$\text{SMLCI}_w = (100 / 3) \times (A/8 + B/4 + C/6)$$

3.6 Coding procedure and quality control

The author coded each system against the codebook and recorded the legal source for every score: bases for scores of 2 are given in the Table 3 notes and bases for scores of 1 in Appendix A. Where the text was ambiguous, the lower score

was assigned. For Bangladesh, the Cyber Security Act 2026, which replaced the Cyber Security Ordinance 2025, and its June 2026 amendment were coded from published legal commentary and official news reports of the enacted text; confirmation against the Bangla gazette text is noted as a limitation in Section 6.2. All coding decisions are reported so that other researchers can reproduce or contest them.

4. Results

The eight legal systems scored between 6 and 15 of a possible 18 on the SMLCI (mean 9.9, median 9.0). The United States scored highest (15; 83.3%) and Bangladesh lowest (6; 33.3%). Across all systems, the Rights and licensing pillar reached 32.8% of its possible maximum, against 75.0% for Transparency and platforms and 70.8% for Liability.

4.1 Legal instruments in the sample

Table 2. Legal systems and principal instruments coded (status as of 20 October 2026)

Legal system	Legal family	Principal instruments coded
European Union (supranational layer)	Supranational	AI Act, Reg. (EU) 2024/1689, art. 50; Directive (EU) 2024/1385, art. 5; Digital Services Act, Reg. (EU) 2022/2065; GDPR
Italy	Civil law	Civil Code art. 10; Law 633/1941 arts. 96–97; Law 132/2025 (Penal Code art. 612-quater, in force 10 October 2025)
United Kingdom	Common law	Passing off; Online Safety Act 2023; Sexual Offences Act 2003 ss. 66B and 66E–66H (creation offences in force 6 February 2026)
United States	Common law (federal and state)	TAKE IT DOWN Act 2025; Cal. Civ. Code §§ 3344, 3344.1; Cal. Lab. Code § 927; Cal. Gov. Code § 84514; N.Y. Civ. Rights Law § 50-f; Tennessee ELVIS Act 2024; Washington SSB 5886 (2026); Minn. Stat. § 609.771
China	Socialist civil law	Civil Code arts. 994, 1019, 1023; Deep Synthesis Provisions (2023); AI-Generated Synthetic Content Labelling Measures (2025); Criminal Law arts. 246, 266, 364

Legal system	Legal family	Principal instruments coded
South Korea	Civil law	Sexual Crimes Special Act art. 14-2 (amended 2024); Public Official Election Act art. 82-8; Unfair Competition Prevention Act art. 2(1)(l); AI Basic Act (in force 22 January 2026); Personal Information Protection Act
India	Common law	Constitution art. 21; Delhi High Court personality-rights orders; IT Act 2000 ss. 66C, 66D, 66E, 67, 67A; IT Amendment Rules 2026 (in force 20 February 2026)
Bangladesh	Common law	Copyright Act 2023; Cyber Security Act 2026 (replacing the Cyber Security Ordinance 2025), s. 25; Cyber Security (Amendment) Act 2026 (passed 30 June 2026) on removal of harmful AI-generated content; Pornography Control Act 2012; Penal Code 1860 s. 499

4.2 Coding results

Table 3. SMLCI coding matrix, ordered by total score (0 = absent, 1 = partial, 2 = explicit)

Legal system	D1	D2	D3	D4	D5	D9	D6	D7	D8	Total (0–18)	Raw %	Pillar-weighted %
United States	2	0	2	2	1	2	2	2	2	15	83.3	83.3
China	2	0	2	1	2	2	2	1	1	13	72.2	76.4
Italy	1	1	1	1	2	1	1	2	2	12	66.7	69.4
South Korea	1	0	1	0	2	1	1	2	2	10	55.6	61.1
United Kingdom	1	0	1	0	0	2	1	2	1	8	44.4	47.2
India	1	0	0	0	2	2	1	1	1	8	44.4	54.2
European Union (layer)	0	0	1	0	2	1	1	2	0	7	38.9	45.8
Bangladesh	0	0	0	0	0	2	1	2	1	6	33.3	38.9

Notes. D1–D4 = Pillar A; D5 and D9 = Pillar B; D6–D8 = Pillar C (Table 1). Principal bases for scores of 2: **US** — state digital-replica statutes (D1, D6), Cal. Lab. Code § 927 (D3), N.Y. Civ. Rights Law § 50-f (D4), TAKE IT DOWN Act (D7, D9), Minn. Stat. § 609.771 (D8); D5 = 1 because disclosure duties are limited to state election-advertising laws such as Cal. Gov. Code § 84514. **China** — Civil Code art. 1019 (D1, D6), Deep Synthesis Provisions consent and platform duties (D3, D9), Labelling Measures (D5). **Italy** — AI Act art. 50 (D5), Penal Code art. 612-quater (D7, D8); portrait consent sits inside copyright law, so D2 = 1. **South Korea** — AI Basic Act (D5), Sexual Crimes Special Act art. 14-2 (D7), Election Act art. 82-8 (D8). **UK** — Sexual Offences Act ss. 66B, 66E (D7), Online Safety Act priority-offence duties (D9). **India** — IT Amendment Rules 2026 labelling and three-hour removal (D5, D9). **EU** — AI Act art. 50(4) (D5), Directive 2024/1385 art. 5 (D7, binding on member states; transposition due 2027). **Bangladesh** —

Cyber Security Act 2026, s. 25 on AI-generated or edited sexual-harassment content (D7); Cyber Security (Amendment) Act 2026 on removal and blocking of harmful AI-generated content (D9); D8 = 1 because a specific offence for AI-generated defamation or disinformation was still only proposed at the cut-off.

Figure 2. SMLCI scores range from 6 to 15 of 18

Rights and licensing (pillar A) has the lowest share of its maximum in seven of eight systems

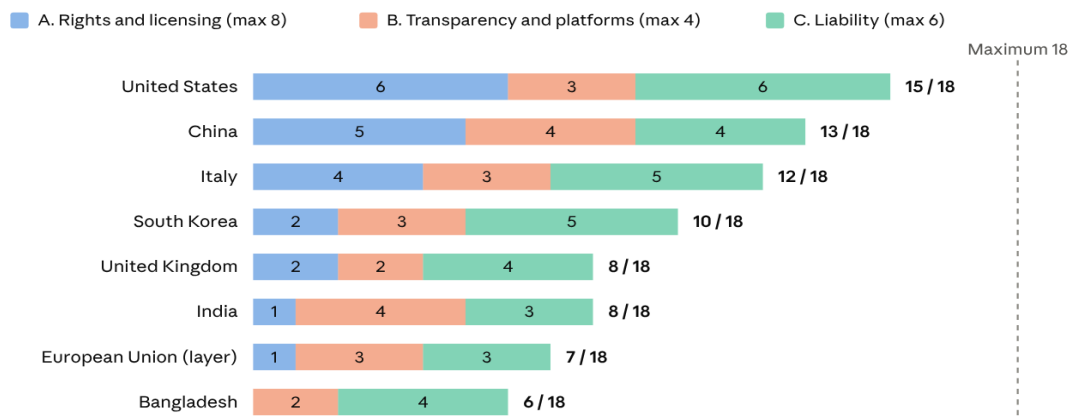


Figure 2. SMLCI score by legal system, split into the three pillars. Numbers inside the bars are pillar scores; source: Table 3.

Ranks were stable under equal pillar weighting. Only the United Kingdom and India changed order, and the Spearman rank correlation between the raw and pillar-weighted indices was $\rho = 0.99$.

Coverage also differed sharply by dimension (Figure 3). Sexual-deepfake offences (D7) reached 87.5% of the possible maximum, while IP or copyright vehicles for likeness (D2) reached 6.3% and post-mortem control (D4) 25.0%.

Figure 3. Sexual-deepfake crimes are near-universal; IP vehicles are rare

Share of the maximum possible score across the eight systems (maximum 16 per dimension)

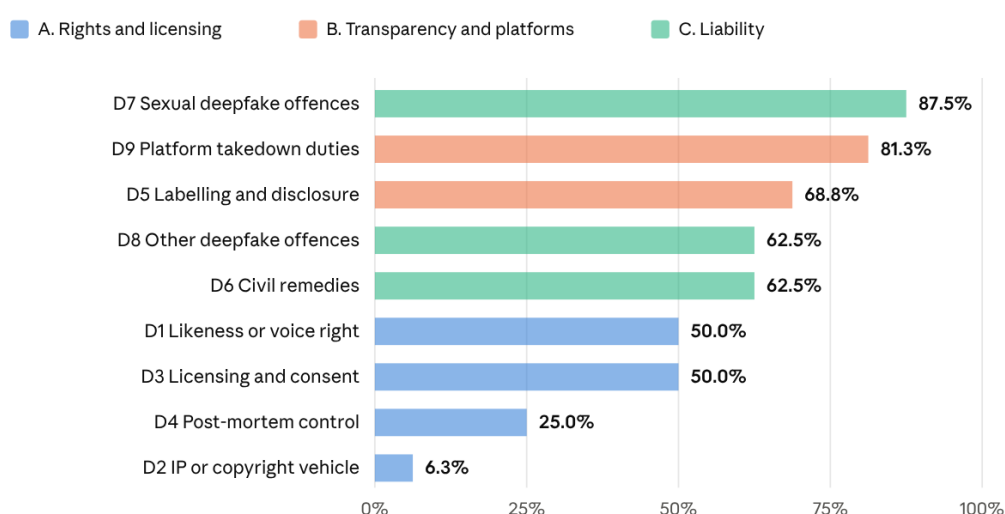


Figure 3. Coverage of each SMLCI dimension, as a share of the maximum score of 16 (2 points $\times$ 8 systems), coloured by pillar; source: Table 3.

4.3 Allocation of liability by actor

Table 4. Who is liable for a harmful deepfake? Main legal exposure by actor

Legal system	Creator or requester	Distributor	Platform	AI provider or tool maker
European Union	Member states must criminalise producing sexual deepfakes (Dir. 2024/1385)	Criminal (same Directive)	DSA notice-and-action	AI Act: providers mark outputs; deployers disclose deepfakes
Italy	Not criminal unless disseminated	Criminal, 1–5 years (art. 612-quater)	DSA notice-and-action	AI Act duties
United Kingdom	Criminal to create or request a sexual deepfake (ss. 66E–66H)	Criminal (s. 66B)	Online Safety Act proactive duties	No specific duty
United States	Civil liability under state statutes	Federal crime to publish intimate digital forgeries	Removal within 48 hours of a valid request	Tennessee: liability for tools whose primary purpose is unauthorised replicas
China	Civil liability (Civil Code art. 1019)	Administrative and general criminal liability	Content-management and labelling duties	Consent, labelling and verification duties
South Korea	Criminal to create; possession and viewing also criminal since 2024	Criminal	General illegal-content duties	AI Basic Act labelling duties
India	General IT Act and penal offences	General IT Act and penal offences	Labelling and three-hour removal duties	Must label synthetic outputs (IT Rules 2026)
Bangladesh	Criminal where content is used for sexual harassment, blackmail or sextortion (s. 25)	Criminal (Cyber Security Act 2026, s. 25)	Removal and blocking of harmful AI-generated content via the regulator (2026 amendment)	No specific duty

Creation alone is criminalised for sexual deepfakes in the United Kingdom and South Korea, and must be criminalised by EU member states. Distribution is criminal in all eight systems, through either specific or general offences. Specific duties for AI providers or tool makers appear in six systems (EU, Italy, US at state level, China, South Korea and India), and are absent in the United Kingdom and Bangladesh.

4.4 IP-style likeness-right models

Table 5. Four models that treat likeness as a property or IP-style right

Feature	Denmark (Bill L 49)	Cyprus (Law 29(I)/2026)	United States (NO FAKES Act 2026)	Tennessee (ELVIS Act 2024)
Status, 20 Oct 2026	Bill; retabled 8 October 2026 after an earlier version lapsed at the general election	Enacted March 2026	Bill S. 4591; placed on the Senate calendar 24 June 2026	In force since 1 July 2024
Legal vehicle	New provisions in the Copyright Act	New sui generis right in the Copyright and Related Rights Law	New federal IP right outside copyright	Statutory property right in name, voice and likeness
Who is protected	All natural persons; performers separately	Natural persons and performers	Every individual	Every individual
Licensing and transfer	Consent required; publishers must be able to prove consent	Law largely silent; commentators read the right as transferable	Licences must be written, describe intended uses and last no more than 10 years for living persons	Assignable and licensable property right
Core prohibition	Making realistic digital imitations available without consent	Making deepfake imitations available without consent	Producing or distributing unauthorised replicas	Unauthorised use of voice or likeness, including AI imitation
Platform mechanism	General EU platform rules (DSA) apply	Not specified in the law	Notice-and-takedown, staydown and counter-notice; safe harbour	None specific

Three of the four models (Denmark, Cyprus and NO FAKES) build an IP-style right with consent as its trigger; only the U.S. bill sets binding rules on licence form and duration. Neither European model is yet tied to a dedicated platform procedure, while the U.S. bill copies and extends the DMCA takedown model.

5

. Discussion

The central finding is an imbalance: legal systems now punish and remove harmful deepfakes far more completely than they define who owns a likeness and how it may be licensed. Platform and liability rules reached about 71–75% of their possible coverage, but rights and licensing rules reached only 33%. Law has therefore built the stick before the property rule that should tell people what is lawful in the first place.

5.1 Copyright is not the main vehicle for identity (RQ1)

Only one of eight systems scored on the IP-vehicle dimension, and only partially (Italy, whose portrait rules happen to sit inside its copyright statute). This confirms the doctrinal view that copyright cannot protect a face or voice because neither is an original work (Infopaq, 2009; Meskys et al., 2020). It also matches the human-authorship line in U.S. law, which leaves AI output itself outside copyright (Thaler v. Perlmutter, 2025; U.S. Copyright Office, 2024).

The Danish and Cypriot initiatives should be read in this light. They use copyright legislation as a *container* for a new right, chiefly to borrow familiar notice-and-takedown and remedy machinery, not because a likeness is a work. The risk, noted in Section 2.2, is that an assignable IP-style right can be bought up by studios or platforms, leaving the person depicted with less control than a non-transferable dignity right would give. Table 5 shows that only the U.S. NO FAKES bill limits licences by form and duration, which is the safeguard this risk calls for.

5.2 Licensing and post-mortem rules are the weakest link (RQ2)

Specific rules on consent and contracts for digital replicas exist only in the United States (California's Labor Code § 927) and China (separate consent for editing biometric features). Post-mortem control covering digital replicas exists clearly only in the United States, through statutes such as New York's § 50-f. India's courts have even held that personality rights are not inheritable (Krishna Kishore Singh v. Sarla A. Saraogi, 2023), so the estates of Indian public figures have no clear claim against posthumous deepfakes.

This matters because the legitimate market for synthetic performers, voice models and dubbing depends on licences that are clear, specific and revocable (Kietzmann et al., 2020). Where licensing rules are absent, two bad outcomes compete: creators cannot be sure a licence is valid, and weaker parties can sign away their likeness in broad, perpetual terms. Rothman (2018) identified the same problem in U.S. publicity law; the results show it is now a global problem.

5.3 Liability is criminal-first and sex-first, and is shifting to platforms (RQ3)

Sexual-deepfake offences were the most widely covered dimension (87.5%). This reflects the evidence that intimate imagery is the dominant harm (Ajder et al., 2019) and the normative argument that such content wrongs the victim even when no viewer is deceived (Öhman, 2020).

Non-sexual deepfakes, such as fraud, impersonation and political manipulation, are covered less consistently and often only through general offences.

The frontier has moved from distributors to two new targets. First, the United Kingdom and South Korea now criminalise *creating* a sexual deepfake, not only sharing it. Second, platforms and tool makers carry growing duties: a 48-hour removal duty in the United States, a three-hour duty in India, proactive duties under the UK Online Safety Act, and labelling duties for AI providers in the EU, China, South Korea and India. This vindicates the prediction of Chesney and Citron (2019) that intermediaries, not anonymous creators, would become the practical point of control.

5.4 Equal totals, different regulatory logics

Totals hide very different designs. The United Kingdom and India both scored 8, but the UK relies on criminal law and platform duties with no labelling rule, while India relies on labelling and takedown with weak criminal and rights coverage. China and the United States score highest for opposite reasons: China through administrative control of providers and platforms, the United States through property-style publicity rights and private litigation. The EU layer scores low on its own because it leaves rights and most criminal law to member states, as Italy's higher score shows.

These results suggest two broad models. A **property-and-market model** (United States, Denmark, Cyprus) treats likeness as an asset that can be licensed and enforced by its owner. A **dignity-and-control model** (China, the EU, South Korea) treats synthetic media as a risk to be labelled, supervised and punished. Each has a blind spot: the first can commodify identity, and the second can concentrate censorship power in the state or platforms.

5.5 Bangladesh: criminalisation without entitlement (RQ4)

Bangladesh shows the starkest imbalance: 4 of 6 possible liability points and 2 of 4 platform

points, but no rights or licensing coverage at all. A person whose face is cloned for an advertisement, or whose voice is used without consent in a non-sexual context, has no clear civil claim, while broadly drafted cyber offences and new content-removal powers remain available to the state. The Cyber Security Act 2026 and its June 2026 amendment on harmful AI-generated content add criminal and removal powers but no entitlement (Bangladesh Sangbad Sangstha, 2026), and a further amendment proposed in 2026 would extend criminal liability to AI-generated rumours, disinformation and defamatory content (Prothom Alo, 2026). The comparative evidence points instead toward a balanced, layered regime, set out in Section 6.

5.6 Theoretical implications

The study adds three points to the literature. First, it shows empirically that the copyright-versus-personality debate is largely settled in practice in favour of personality and publicity rights, with IP-style rights emerging only as enforcement containers. Second, it reframes deepfake regulation as a problem of *pillar balance*: a regime is only as strong as its weakest pillar. Third, the SMLCI offers a transparent, replicable tool that future studies can extend to more jurisdictions and update as laws change.

6.1 A layered model for jurisdictions without a dedicated regime

The results support a four-layer regime that balances all three pillars (Figure 4). It is designed for Bangladesh but applies to any jurisdiction that currently relies mainly on cyber-crime law.

1. **Rights layer.** Enact a statutory, non-waivable personality right over face, body and voice that expressly covers digital replicas. Ground it in dignity rather than copyright, so that the core right cannot be sold outright.
2. **Licensing layer.** Allow use of a likeness only under a written licence that describes each intended use, has a fixed maximum term and can be revoked for future uses. Give estates a fixed-term post-mortem right, following the U.S. and Danish approaches.
3. **Transparency and platform layer.** Require providers to mark synthetic outputs and platforms to label them, as in the EU AI Act and India's 2026 rules. Add a notice-and-takedown procedure with a short deadline, a counter-notice and penalties for bad-faith notices.
4. **Liability layer.** Keep narrowly drafted offences for sexual deepfakes (including creation), fraud and election manipulation, and add a civil claim for damages and injunctions. Protect satire, parody, news reporting and research through express exceptions, as Denmark's bill and the NO FAKES Act d

Figure 4. Proposed regime: right and licence first, then takedown and sanction

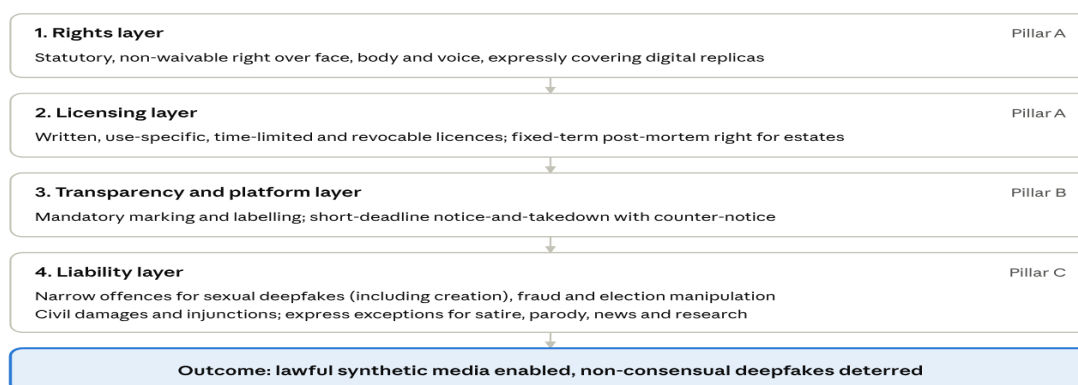


Figure 4. Proposed layered regime, built from the comparative results; each layer maps onto a pillar of Figure 1. Source: authors' proposal.

6.2 Limitations

The study has four limitations. First, the SMLCI measures the presence of law on the books, not enforcement or effectiveness; a high score does not prove that victims obtain remedies. Second, ordinal coding compresses complex rules into three levels, and the unweighted index assumes that each dimension matters equally, although the robustness check suggests rankings are stable. Third, coding was carried out by a single researcher and relied partly on translations and legal commentary, particularly for China, South Korea and Bangladesh; independent second coding and confirmation against original-language texts would strengthen reliability. Fourth, the field changes monthly: Denmark's bill, the NO FAKES Act and Bangladesh's proposed amendments could alter the scores soon after the 20 October 2026 cut-off.

6.3 Future research

Future work should (a) add a second coder and report inter-coder agreement, (b) extend the index to more Global South jurisdictions, (c) link SMLCI scores to enforcement data such as takedown volumes and prosecutions, and (d) study how creators, performers and platforms actually negotiate digital-replica licences.

6.4 Conclusion

Deepfake law has matured quickly, but unevenly. Across eight legal systems, criminal and platform rules now cover most serious harms, while the rules that decide who owns a likeness, how it may be licensed and what happens after death remain

thin. Copyright is not, and should not become, the main home of identity protection; its value lies in the enforcement tools it can lend to a dignity-based personality right. The take-home message for legislators, especially in Bangladesh and other countries still relying on cyber-crime law, is clear: **build the right and the licence first, then the takedown and the sanction**, so that the law deters non-consensual deepfakes without blocking the lawful creative economy of synthetic media.

Declarations

Funding. This research received no specific grant from any funding agency.

Conflict of interest. The author declares no conflict of interest.

Ethics statement. Not applicable; the study analyses publicly available legal sources and involves no human participants.

Data availability. All coding decisions and their legal bases are reported in Table 3 and Appendix A; the coding spreadsheet is available from the corresponding author on reasonable request.

Author contributions (CRediT). [Author name]: Conceptualization, Methodology, Formal analysis, Investigation, Visualization, Writing – original draft, Writing – review and editing.

Use of AI tools. Generative AI tools were used to assist with drafting and language editing. The author reviewed and verified all content and legal sources and takes full responsibility for the work.

References

Books, articles and reports

- Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The state of deepfakes: Landscape, threats, and impact*. Deepttrace.
- Bangladesh Sangbad Sangstha. (2026, June 30). *Cyber Security Amendment Bill, 2026 passed in JS*. <https://www.bssnews.net/js-session/401310>
- 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>
- Delfino, R. A. (2019). Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic act. *Fordham Law Review*, 88(3), 887–938.

- Ginsburg, J. C., & Budiardjo, L. A. (2019). Authors and machines. *Berkeley Technology Law Journal*, 34(2), 343–456.
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27, 2672–2680.
- Gosse, C., & Burkell, J. (2020). Politics and porn: How news media characterizes problems presented by deepfakes. *Critical Studies in Media Communication*, 37(5), 497–511. <https://doi.org/10.1080/15295036.2020.1832697>
- 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>
- Meskys, E., Kalpokienė, J., Jurcys, P., & Liaudanskas, A. (2020). Regulating deep fakes: Legal and ethical considerations. *Journal of Intellectual Property Law & Practice*, 15(1), 24–31. <https://doi.org/10.1093/jiplp/jpz167>
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), Article 7. <https://doi.org/10.1145/3425780>
- Öhman, C. (2020). Introducing the pervert's dilemma: A contribution to the critique of deepfake pornography. *Ethics and Information Technology*, 22(2), 133–140.
- Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society Research Institute.
- Prothom Alo. (2026). *Cyber Security (Amended) Act: 10 years' imprisonment for spreading rumours, disinformation*. <https://en.prothomalo.com/bangladesh/wbq9kji6z7>
- Rothman, J. E. (2018). *The right of publicity: Privacy reimagined for a public world*. Harvard University Press.
- Samuelson, P. (2023). Generative AI meets copyright. *Science*, 381(6654), 158–161. <https://doi.org/10.1126/science.adi0656>
- Siems, M. M. (2005). Numerical comparative law: Do we need statistical evidence in law in order to reduce complexity? *Cardozo Journal of International and Comparative Law*, 13(2). <https://larc.cardozo.yu.edu/cjicl/vol13/iss2>
- Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, 64, 131–148. <https://doi.org/10.1016/j.inffus.2020.06.014>
- S. Copyright Office. (2024). *Copyright and artificial intelligence, Part 1: Digital replicas*. <https://www.copyright.gov/ai/>
- 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>
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 40–53. <https://doi.org/10.22215/timreview/1282>
- Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law* (T. Weir, Trans.; 3rd ed.). Clarendon Press.

Cases

- Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi High Court, 20 September 2023).
- Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).
- Infopaq International A/S v. Danske Dagblades Forening, Case C-5/08, EU:C:2009:465 (CJEU, 16 July 2009).
- Irvine v. Talksport Ltd [2002] EWHC 367 (Ch).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Krishna Kishore Singh v. Sarla A. Saraogi & Ors., CS(COMM) 187/2021, 2023 SCC OnLine Del 3997 (Delhi High Court, 11 July 2023).

Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988).

Thaler v. Perlmutter, 130 F.4th 1039 (D.C. Cir. 2025).

Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977).

Legislation and bills

Bangladesh. Copyright Act, 2023. Cyber Security Ordinance, 2025 (in force 21 May 2025; replaced in 2026). Cyber Security Act, 2026, s. 25. Cyber Security (Amendment) Act, 2026 (passed 30 June 2026). Pornography Control Act, 2012. Penal Code, 1860, s. 499.

China. Civil Code of the People's Republic of China (2020), arts. 994, 1019, 1023. Cyberspace Administration of China et al., Provisions on the Administration of Deep Synthesis of Internet-Based Information Services (in force 10 January 2023). Cyberspace Administration of China et al., Measures for Labelling Artificial Intelligence-Generated Synthetic Content (in force 1 September 2025). Criminal Law of the People's Republic of China, arts. 246, 266, 364.

Cyprus. Law 29(I)/2026 amending the Copyright and Related Rights Law 59/1976. Commentary consulted: [Kluwer Copyright Blog](#).

Denmark. Bill L 49 (2026–27) amending the Copyright Act, tabled 8 October 2026. Summary consulted: [PPC Land](#).

European Union. Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016. Regulation (EU) 2022/2065 (Digital Services Act), OJ L 277, 27.10.2022. Directive (EU) 2024/1385 on combating violence against women and domestic violence, OJ L, 2024/1385, 24.5.2024. Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

India. Constitution of India, art. 21. Information Technology Act, 2000, ss. 66C, 66D, 66E, 67, 67A. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (notified 10 February 2026; in force 20 February 2026).

Italy. Civil Code, art. 10. Law No. 633 of 22 April 1941 (Copyright Law), arts. 93, 96–97. Law No. 132 of 2025 on artificial intelligence, inserting Penal Code art. 612-quater (in force 10 October 2025).

South Korea. Act on Special Cases Concerning the Punishment of Sexual Crimes, art. 14-2 (as amended 2024). Public Official Election Act, art. 82-8. Unfair Competition Prevention and Trade Secret Protection Act, art. 2(1)(l) (in force 20 April 2022). Framework Act on the Development of Artificial Intelligence and the Establishment of a Foundation for Trust (AI Basic Act), art. 31 (in force 22 January 2026). Personal Information Protection Act.

United Kingdom. Online Safety Act 2023, c. 50. Sexual Offences Act 2003, ss. 66B, 66E–66H. Data (Use and Access) Act 2025, s. 138 (in force 6 February 2026).

United States (federal). TAKE IT DOWN Act, Pub. L. No. 119-12 (2025). NO FAKES Act of 2026, S. 4591, 119th Cong. (2026).

United States (states). Cal. Civ. Code §§ 3344, 3344.1. Cal. Gov. Code § 84514. Cal. Lab. Code § 927. Minn. Stat. § 609.771. N.Y. Civ. Rights Law § 50-f. Ensuring Likeness, Voice, and Image Security (ELVIS) Act of 2024, Tenn. Code Ann. § 47-25-1101 et seq. (in force 1 July 2024). Substitute Senate Bill 5886, 69th Leg., 2026 Reg. Sess. (Wash. 2026).

Appendix A. Bases for partial (score 1) codes

Legal system	Dimension scored 1	Legal basis
United States	D5	State election-advertising disclosure laws, e.g. Cal. Gov. Code § 84514
China	D4	Civil Code art. 994 (close relatives may protect a deceased person's portrait, name and reputation)
China	D7, D8	General offences: Criminal Law arts. 364 (obscene materials), 246 (defamation), 266 (fraud)
Italy	D1, D2, D3, D4	Civil Code art. 10; Law 633/1941 arts. 93, 96–97 (portrait consent, including relatives after death)
Italy	D6, D9	General civil remedies; DSA notice-and-action
South Korea	D1	Unfair Competition Prevention Act art. 2(1)(l) (widely known persons, commercial use only)
South Korea	D3, D6, D9	Personal Information Protection Act consent; general tort and unfair-competition remedies; general illegal-content duties
United Kingdom	D1, D6	Passing off (Irvine v. Talksport, 2002); misuse of private information; defamation
United Kingdom	D3, D8	UK GDPR consent for biometric data; Fraud Act 2006 and general communications offences
India	D1, D6	Judge-made personality rights and injunctions (Anil Kapoor, 2023; Puttaswamy, 2017)
India	D7, D8	IT Act 2000 ss. 66E, 67, 67A; ss. 66C, 66D
European Union	D3, D6, D9	GDPR consent for biometric data and compensation; DSA notice-and-action
Bangladesh	D6, D8	General defamation and tort remedies; Penal Code s. 499 and general offences under the Cyber Security Act 2026