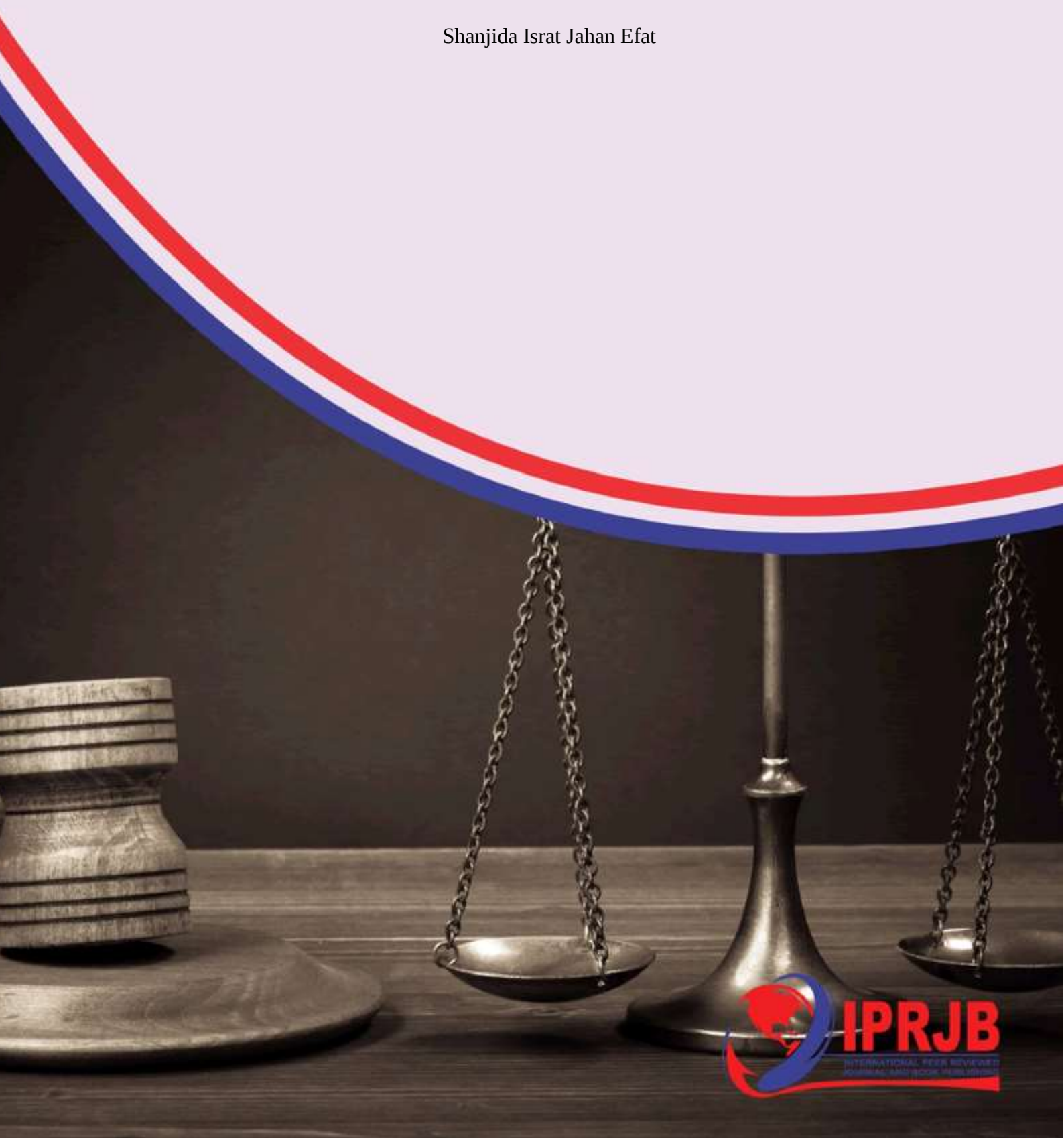
International Journal of
Law and Policy
(IJLP)

Personality Rights, Detection Bias and Effective Remedies for AI-Generated Identity Harm: A Comparative Study of India and Bangladesh

Shanjida Israt Jahan Efat



International Journal of Law and Policy
ISSN 2520-4637 (online)
Vol.11, Issue 1, No.1. pp 1 – 25, 2026

www.iprjb.org

Personality Rights, Detection Bias and Effective Remedies for AI-Generated Identity Harm: A Comparative Study of India and Bangladesh

Shanjida Israt Jahan Efat
Assistant Professor, Department of Law, Notre Dame University, Bangladesh

Article History

Received 13th May 2026

Received in Revised Form 19th June 2026

Accepted 16th July 2026

How to cite in APA format:

Efat, S. (2026). Personality Rights, Detection Bias and Effective Remedies for AI-Generated Identity Harm: A Comparative Study of India and Bangladesh. *International Journal of Law and Policy*, *11*(1), 1–25. https://doi.org/10.47604/ijlp.3876

Abstract

Purpose: This article examines whether an automatic personality right in face, voice, likeness and synthetic performance can provide an effective remedy for ordinary victims of AI-generated identity harm in India and Bangladesh. It defines effectiveness by accessibility, speed, practical outcomes and independence from celebrity or market value.

Methodology: The study uses doctrinal, comparative and law-and-technology analysis of cases, legislation, platform regulation, human-rights standards and technical research reviewed through 15 July 2026. India is examined as the more developed regional common-law and constitutional personality-rights jurisdiction, while Bangladesh is used to test institutional feasibility in a lower-resource and speech-sensitive setting.

Findings: An automatic right is necessary but insufficient. Celebrity litigation establishes important commercial and dignitary principles, yet ordinary victims face anonymous distribution, litigation cost, stigma, platform opacity and detector error. Bengali audio evidence and demographic-fairness research show that technical detection can become an unequal gateway to legal proof. A 53% accurate detector cannot fairly determine access to preservation or interim relief.

Unique Contribution to Theory, Practice and Policy: The article shifts the debate from ownership to remedy design and connects detector bias directly to evidence, equality and institutional access. It proposes a judicially supervised Digital Identity Remedy Cell within the legal-aid system rather than an executive censorship authority. Bangladesh should adopt a narrow civil AI Identity Harm Act triggered by synthetic identification rather than fame. It should require rapid platform preservation and disclosure, graduated proof thresholds, audited local-language tools, anonymised dockets, in-camera hearings, distinct commercial and dignitary remedies, and clear speech defences with explicit burdens of production.

Keywords: *Personality Rights, Deepfakes, Digital Replicas, Detection Bias, Effective Remedy, Synthetic Identification, Bangladesh, India*

JEL Classification Codes: *K24, K42, O33, D63*

INTRODUCTION

The concept of ownership in this article is not used in a crude property sense. A person should not control every public reference to their face or voice, because democratic life requires quotation, criticism, journalism, memory and cultural reference. The relevant distinction is between reference and replacement. Reference places a person within public discourse. Synthetic replacement makes the person appear to speak, sing, endorse, perform, participate in politics, or appear in intimate material without consent. The proposed right is therefore triggered by synthetic identification, not by fame, market value or mere recognisability.

That distinction is especially important for legal journals because the deepest challenge is not novelty but allocation. The legal system must allocate the risk of uncertainty among victims, platforms, uploaders and the state. If the victim bears every uncertainty, the right is symbolic. If platforms must remove every contested item without process, speech suffers. If the state controls the definition of harmful synthetic content without safeguards, deepfake law becomes another speech-control instrument. The article's proposal is therefore deliberately procedural: it designs stages, burdens and safeguards rather than announcing an absolute proprietary dominion over identity.

The article also avoids the assumption that more criminal law automatically means more protection. Criminalisation may express social condemnation, but it often arrives too late for viral media and can be selectively enforced. A remedy-centred approach asks what the victim needs first: safety, preservation, removal, correction, anonymity and accessible adjudication. Punishment remains available for serious or repeated abuse, but it is not the organising principle of the whole field. That distinction should guide every later drafting choice.

Generative artificial intelligence has changed the practical meaning of identity. A short voice sample can become a singing model; a photograph can become a false endorsement; and a video fragment can become a fabricated political speech. The resulting injury may be commercial, but it may also concern dignity, autonomy, safety, sexual privacy, evidence and democratic trust. Commercial identity harm concerns the unauthorised exploitation of a persona’s market value. Dignitary identity harm concerns the non-consensual attribution of speech, conduct, intimacy or affiliation to a person. These heads of harm overlap, but neither should be treated as a prerequisite for the other.

Recent Indian litigation demonstrates both rapid doctrinal development and the continuing importance of celebrity claims. The Bombay High Court restrained AI-generated voice models and unauthorised commercial imitation in *Arijit Singh v. Codible Ventures LLP* (2024) and *Asha Bhosle v. Mayk Inc.* (2025). The Delhi High Court protected name, image, voice, likeness and other indicia of persona in *Anil Kapoor v. Simply Life India* (2023) and treated AI chatbots and deepfake videos as capable of violating both commercial personality interests and dignity in *Aishwarya Rai Bachchan v. Aishwaryaworld.com* (2025). In 2026, the Delhi High Court continued this line in *Varun Dhawan v. Artist Booking Company* (2026) and *Ravindra Shukla alias Ravi Kishan v. Ashok Kumar (John Doe)* (2026), including orders directed at AI-generated and pornographic impersonation.

These celebrity cases should not be discounted. They establish that unauthorised AI imitation can injure both market-facing persona and personal dignity, and they supply useful models for urgent injunctions and orders against unknown defendants. They nevertheless involve a class of claimant with exceptional recognisability, comparison material, legal resources and access to higher courts. Ordinary victims commonly face a different remedial problem: anonymous uploaders, closed messaging groups, weak local-language detection, inability to finance expert evidence, and fear that public proceedings will intensify stigma. The distinction is therefore not between worthy and unworthy victims, but between different harm profiles and different capacities to activate the law.

This article asks whether a personality-rights architecture can become an effective remedy for non-celebrity victims in low-resource and unevenly digitised jurisdictions. An effective remedy is defined here as one that is accessible without prohibitive cost, available quickly enough to limit viral harm, capable of securing preservation, removal, correction, compensation or protection as appropriate, and not conditioned on celebrity status or measurable market value. The article argues that an automatic right is necessary but insufficient unless it is joined to platform-side preservation and disclosure duties, graduated evidentiary thresholds, dignitary remedies, independent review and audited Bengali and South Asian detection infrastructure.

Problem Statement

Existing personality-rights doctrine offers its strongest relief where harm is commercially legible and the claimant can reach a superior court quickly. That model does not adequately address the ordinary victim whose injury is primarily dignitary, whose evidence is held by a platform, whose language is poorly represented in forensic benchmarks, and whose decision to complain is constrained by both stigma and cost. Bangladesh's large court backlog, uneven access to legal aid and history of overbroad cyber-law enforcement intensify these barriers. The beneficiaries of a better architecture are therefore not only victims. Courts gain clearer evidentiary thresholds; platforms gain defined duties and safe harbours; legal-aid providers gain a triage pathway; regulators gain auditable standards; and journalists and civil society gain speech safeguards.

Research Questions

The article is organised around four research questions.

i. First, can an automatic personality right in face, voice and likeness provide an effective remedy for ordinary victims of AI identity harm, or does it mainly strengthen already powerful celebrity claimants?
ii. Secondly, how does detection bias in AI-forensic systems transform the legal analysis of proof, equality and access to justice?
iii. Thirdly, what does Indian personality-rights jurisprudence reveal about the promise and limits of a constitutional route to AI identity protection?
iv. Fourthly, what remedial architecture should Bangladesh adopt if it wishes to protect identity without reproducing the speech-control problems associated with digital-security law?

Objectives

The objectives are fivefold. The first is descriptive: to reconstruct the current convergence in scholarship and reform around automatic, unwaivable personality rights. The second is doctrinal: to identify how Indian courts have used privacy, passing off and publicity concepts to restrain AI-enabled identity appropriation. The third is comparative: to test that model against Bangladesh's constitutional text, cyber-law history, judicial capacity and low-resource language environment. The fourth is critical: to show that detection bias is not merely a technical weakness but a condition determining whose rights become legally provable. The fifth is normative: to propose a remedy design combining personality rights, platform obligations, evidence rules, anonymity protection, exceptions for public-interest expression, and audited detection infrastructure.

Argument and Contribution

The article makes three contributions. First, it shifts the debate from right creation to remedy design. A right that cannot be triggered, proved or enforced by the ordinary victim is not a meaningful right, even if it is beautifully drafted. Secondly, it links legal equality with technical detection. Where language and demographic characteristics affect the reliability of forensic tools, the legal system's evidentiary gateway is unequal. Thirdly, it uses Bangladesh not as a peripheral example but as a stress test for global reform: if a proposed right cannot operate in Bangladesh, it is not a general solution for the Global South.

LITERATURE REVIEW

The United Kingdom’s privacy cases show why a dignity route is useful but incomplete for AI identity harm. *Kaye v. Robertson* (1991) exposed the absence of a general privacy remedy before the Human Rights Act, while *Campbell v. MGN Ltd.* (2004) and *Douglas v. Hello! Ltd.* (2007) developed misuse-of-private-information balancing. Those doctrines remain insufficient where the contested media is wholly synthetic, derived from public source material, and does not reveal a true private fact. They may protect secrecy or confidence, but they do not directly address the replacement of a person’s communicative agency, the preservation of platform evidence, or the speed of repeat uploading.

Studies of computational propaganda and recent election deepfake research show that the political risk is not hypothetical: synthetic media interacts with coordinated distribution, platform incentives and audience uncertainty (Bradshaw & Howard, 2019; Ranka et al., 2024; Livernoche et al., 2025). Deepfake harms in low-tech environments also raise awareness, access and verification problems that ordinary litigation does not address (Wasi et al., 2025).

A further tension in the literature is the relation between copyright and personhood. Copyright is attractive because it has an enforcement machine: injunctions, notice systems, licensing practices and cross-border vocabulary. But identity is not a work of authorship. The face and voice precede creative fixation, and their value may be intimate rather than commercial. A copyright-adjacent model should therefore borrow mechanisms from copyright without importing copyright's market assumptions wholesale.

A related literature on intimate-image abuse is particularly useful because it shows why consent and context matter more than simple truth or falsity. A genuine intimate image can be harmful when shared without consent; a synthetic intimate image can be harmful even though it is false. The shared wrong is the coercive appropriation of sexual or personal presentation. This insight helps separate AI identity harm from ordinary misinformation. The victim's complaint is not only that the audience is deceived. It is that the victim's body, voice or likeness has been drafted into an unwanted communicative act.

Personality Rights before Generative AI

Personality rights developed through overlapping doctrines rather than through a single universal category. In India, the older path runs through passing off and reputation. DM Entertainment recognised that a famous performer's persona could be commercially misappropriated (*DM Entertainment Pvt. Ltd. v. Baby Gift House*, 2010). Amitabh Bachchan then gave procedural strength to that protection through broad interim relief against unauthorised exploitation of a celebrity's name, image, voice and dialogues (*Amitabh Bachchan v. Rajat Nagi*, 2022). The constitutional strand is connected to privacy and dignity. Puttaswamy confirmed privacy as a fundamental right under Article 21 and placed autonomy, dignity and informational self-determination at the centre of Indian constitutional law (*Justice K. S. Puttaswamy v. Union of India*, 2017). Rajagopal had earlier recognised that the unauthorised publication of private facts and the exploitation of identity can engage constitutional and common-law concerns (*R. Rajagopal v. State of Tamil Nadu*, 1994).

At the same time, Indian law continues to show uncertainty when the claimant is not a living celebrity with market value. Krishna Kishore Singh framed post-mortem claims through goodwill, misrepresentation and damage (*Krishna Kishore Singh v. Sarla A. Saraogi*, 2021). Deepa Jayakumar adopted a more restrictive approach to inheritable personality interests (*Deepa Jayakumar v. A. L. Vijay*, 2021). The disagreement is doctrinally significant, but both cases reveal the same gravitational pull: identity becomes easiest to protect when it can be translated into reputation, goodwill or market loss.

United States publicity law follows a different route but displays a similar tension. Midler and Waits protected distinctive voices against commercial imitation (*Midler v. Ford Motor Co.*, 1988; *Waits v. Frito-Lay, Inc.*, 1992). White extended the right of publicity to evocative indicia of persona (*White v. Samsung Electronics America, Inc.*, 1992). The doctrinal root goes back to Haelan Laboratories, where the Second Circuit recognised a transferable commercial interest in the publicity value of identity (*Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*, 1953). Zacchini constitutionalised part of the debate by balancing publicity rights against the First Amendment (*Zacchini v. Scripps-Howard Broadcasting Co.*, 1977). Later cases such as Comedy III, Cardtoons, Rogers and Keller show the recurring problem: the law must protect identity without suppressing expressive works that comment on, transform or refer to real persons (*Comedy III Productions, Inc. v. Gary Saderup, Inc.*, 2001; *Cardtoons, L.C. v. Major League Baseball Players Association*, 1996; *Rogers v. Grimaldi*, 1989; *Keller v. Electronic Arts, Inc.*, 2013).

The New Convergence: Automatic Personality Rights

Generative AI has accelerated a new scholarly convergence. Bosher argues that deepfakes, digital replicas and human digital twins justify a direct personality right protecting voice, image, name and likeness, including non-commercial uses where the dignitary harm is serious (Bosher, 2026). Chopra, Sony and Chopra describe the normative core as Consent, Compensation and Control (Chopra et al., 2025). Marlan adds a criminal-law dimension for serious generative identity theft (Marlan, 2025). Mahamuni reads the Indian AI cases and the American voice-cloning litigation around Lehrman v Lovo as signs that India requires a dedicated statutory solution rather than piecemeal celebrity litigation (Mahamuni, 2025).

The U.S. Copyright Office's Digital Replicas report similarly concluded that copyright, privacy, tort and publicity law leave important gaps and recommended protection extending beyond commercially valuable identities (U.S. Copyright Office, 2024). Denmark has prepared, but as of the research cut-off had not completed, a copyright-law amendment directed at realistic digital replicas of a person's body, face and voice (Karttunen, 2026; Milmo, 2025). The direction of reform is significant, but the legislative status must not be overstated.

A further remedial model emerged in the United States through the TAKE IT DOWN Act. Its platform obligations, effective from May 2026, require a notice process and rapid removal of covered non-consensual intimate images, including qualifying digital forgeries, together with reasonable efforts concerning known identical copies (TAKE IT DOWN Act, 2025; Federal Trade Commission, 2026). The Act does not solve the broader field of voice, endorsement or political impersonation, but it demonstrates that first-response duties can be specified in hours rather than left to ordinary litigation.

The appeal of the convergence is obvious. A copyright-like right can vest automatically, travel across platforms, support notice-and-takedown, survive death, and use familiar defences for criticism, parody, satire and public-interest reporting. Yet that elegance also hides assumptions. It assumes that the claimant knows that a synthetic artefact exists, can identify a responsible actor, can prove identity linkage, can access a forum, and can withstand the social consequences of litigation. Those assumptions are not doctrinal details; they are the conditions that decide who benefits.

Platform Governance and Transparency

Platform regulation supplies partial correctives. The Digital Services Act provides notice-and-action mechanisms and systemic-risk duties for very large platforms (Regulation [EU] 2022/2065, 2022). Article 50 of the EU AI Act establishes transparency duties for deepfakes and other synthetic content, with the Act's general application scheduled for 2 August 2026 at the research cut-off (Regulation [EU] 2024/1689, 2024; European Commission, 2026). These instruments do not create a universal personality right, but they move part of the remedial burden from the isolated victim to the intermediary that hosts, recommends, monetises or preserves the content.

The literature also distinguishes cultural and structural reasons for low complaint rates. Cultural barriers include sexual stigma, fear of family consequences, reputational blame and community retaliation. Structural barriers include filing costs, lack of legal aid, absence of local technical expertise, platform opacity, slow disclosure and congested courts. The two interact, but they require different remedies: confidentiality and victim-sensitive procedure for the former; subsidised assistance, preservation duties and simplified adjudication for the latter.

Speech-protective constitutional standards remain crucial. Article 10(2) of the European Convention requires restrictions on expression to be prescribed by law and necessary in a democratic society (European Convention on Human Rights, 1950, art. 10[2]). The Canadian Charter's section 1 similarly demands demonstrable justification for limits on rights (Canadian Charter of Rights and Freedoms, 1982, s. 1). A personality-rights regime without an equivalent discipline risks overreach. A state may use the language of deepfake control to suppress parody, investigative journalism or dissent. Remedy design must therefore do two things at once: lower the evidentiary barrier for real victims while making state and elite censorship harder.

Bangladesh and the Underdeveloped Global South Literature

Bangladesh has received less attention in personality-rights scholarship even though it is a critical test of practical effectiveness. The Constitution protects equality, non-discrimination, life and personal liberty, and expression (Constitution of the People's Republic of Bangladesh, 1972). The statutory environment changed again in 2026: the Cyber Security Act 2026 replaced the 2025 ordinance, and the Personal Data Protection Act 2026 created a new data-governance framework. The Information and Communication Technology Act 2006 remains relevant to the cyber-tribunal structure. None of these instruments yet supplies a complete civil, dignity-based remedy for non-consensual synthetic identification.

Bangladesh's earlier digital-security laws attracted sustained criticism for their use against journalists and dissent (Amnesty International, 2024; ARTICLE 19, 2025; Transparency International Bangladesh, 2024). This history creates a design constraint, not an argument against protecting victims. A new law must separate victim-centred civil relief from broad public-order offences, place final decisions under judicial control, and create transparent review of platform and administrative action.

Gaps in the Existing Study

The Celebrity-Case Gap

Reported personality-rights cases are valuable because they establish recognisable causes of action and demonstrate that courts can grant urgent relief. They are nevertheless an imperfect proxy for ordinary victims. Famous claimants possess comparison material, legal resources, commercial markets and public recognisability. Ordinary claimants may be known only to a family, workplace or local political community, yet that limited audience can be the audience in which the harm is most severe. The gap is therefore not the absence of celebrity rights, but the absence of procedures calibrated to non-celebrity proof and loss.

The Commercial-Dignitary Gap

A market-centred framework values lost endorsements, dilution of goodwill and licensing substitution. Those losses are real, but they do not measure fabricated intimacy, family conflict, coercion, political intimidation, school exclusion, employment disruption or safety risk. The existing literature often treats dignity as an additional consideration after commercial liability has been established. A complete framework must recognise commercial identity and dignitary identity as separate interests and allow remedies for either.

The Proof and Detection Gap

The ordinary claimant must often show that a file is synthetic, that it is identity-linked, and that a defendant or platform failed to act. The relevant evidence may include detectors, metadata, upload logs, comparison recordings, provenance signals and expert testimony, most of which are unavailable to the claimant at the moment of complaint. The best reported zero-shot result in a Bengali deepfake-audio benchmark was 53.80% accuracy with a 46.20% equal-error rate, while fairness research shows that visual detectors can distribute error unevenly across demographic groups (Ju et al., 2024; Samu et al., 2025). A right conditioned on a high detector score therefore creates unequal access to legal proof.

The legal answer is not to treat a 53% score as affirmative proof of authenticity or falsity. It is to lower the initial threshold for preservation, shift production of platform-controlled evidence after notice, and reserve final liability for a totality-of-evidence assessment. Technical uncertainty should trigger evidence protection and human review, not dismissal.

The Cultural and Gendered Access Gap

Synthetic intimate and retaliatory media can make public complaint itself dangerous. Sexual stigma, anticipated family consequences, victim blaming and community retaliation are cultural barriers that may deter reporting even where a formal cause of action exists. Named pleadings, open hearings and unrestricted exhibits can then reproduce the harm. Anonymised dockets, in-camera hearings, sealed exhibits and restrictions on republication are therefore substantive parts of an effective remedy, not optional courtroom courtesy.

The Structural Access and Temporal Gap

Structural barriers are different. They include the cost of counsel and experts, weak legal-aid coverage, inability to identify anonymous uploaders, limited local forensic capacity, foreign platform control of evidence and court delay. Bangladesh reported more than 4.6 million pending cases across the judiciary by March 2026, including more than 4 million in lower courts (The Daily Star, 2026). Earlier government reporting also recorded thousands of pending cases across eight cyber tribunals (BSS, 2025). Because screenshots, downloads and reposts can multiply within hours, a remedy must be evaluated by what happens in the first forty-eight hours, not only by the final judgment.

The Bangladesh Regulatory-Design Gap

Bangladesh's current framework addresses cyber offences and personal-data governance but does not yet integrate a narrow civil right against synthetic identification, platform preservation, evidentiary burden shifting, victim confidentiality, audited detection and speech-protective review. Policy research has identified accountability and governance gaps, and recent scholarship argues for movement beyond criminalisation (Khan, 2026; Tech Global Institute, 2024). The unresolved task is to combine these strands into an administratively feasible architecture that cannot easily be converted into a general censorship mechanism.

METHODOLOGY

This study uses a qualitative doctrinal, comparative and law-and-technology methodology, with sources reviewed through 15 July 2026. Doctrinal analysis examines constitutional provisions, statutes, regulations and reported decisions concerning privacy, publicity, passing off, dignity, equality, intermediary duties, evidence and freedom of expression. The comparison is purposive: India has a more developed body of common-law and constitutional personality-rights jurisprudence, together with 2026 intermediary rules for synthetically generated information, while Bangladesh has an emerging cyber-security and data-protection framework but less developed civil doctrine and weaker remedial capacity. The comparison is functional rather than transplant-oriented. It traces the steps an ordinary victim must complete to discover content, report it, preserve data, establish identity linkage, obtain platform disclosure, answer defences, secure relief and enforce an order. Technical literature is used as legal evidence about reliability, demographic and language variation, provenance and documentation, not as an independent evaluation of any commercial detector (Barocas & Selbst, 2016; Buolamwini & Gebru, 2018; Gebru et al., 2021; Ju et al., 2024; Mirsky & Lee, 2021; Mitchell et al., 2019; Raji & Buolamwini, 2019; Samu et al., 2025). Equality, sexual-privacy and epistemic-harm scholarship supplies the normative framework for distinguishing market loss from dignitary, relational and democratic harm (Chesney & Citron, 2019; Citron, 2019; Citron & Franks, 2014; Rini, 2020). The study does not claim a representative dataset of Bangladeshi complaints, validate a detector or draft a complete statute. Its output is a minimum remedial architecture against which future legislation and empirical work can be tested.

Research Question One: Can Automatic Personality Rights Provide an Effective Remedy for Ordinary Victims?

The strongest case for an automatic right is that consent cannot be made meaningful if the claimant must first prove market value. AI systems can appropriate a face or voice before any negotiation, and the output can spread before the claimant even knows it exists. Registration would be unrealistic for ordinary people and would perversely protect the already organised. Automatic vesting therefore matters because personhood should not depend on administrative foresight.

The strongest objection to a property-like right is overbreadth. People appear in public affairs, art, history, comedy and news. A law treating every recognisable depiction as controlled use would chill legitimate expression. The proposed trigger is therefore non-consensual synthetic identification: a materially generated or manipulated output that causes a reasonable audience to attribute speech, action, endorsement, intimacy, political affiliation or other identity-linked conduct to the claimant. The trigger is independent of fame and commercial value. Mere reference, quotation or depiction remains outside the right unless the work substitutes for the person in a deceptive or materially harmful way.

The remedy should also recognise collective and democratic harms without allowing the state to monopolise enforcement. A fabricated political video harms the person impersonated, but it may also harm voters and the integrity of public debate. The safest response is not a broad public-order offence. It is a combination of individual complaint rights, platform labelling duties, election-period transparency rules and independent oversight. That approach protects democracy while reducing incentives for partisan misuse.

Why the Right is Necessary

The first research question begins with necessity. Existing doctrines do not fully capture AI identity harm. Defamation requires a false statement and reputational damage. Privacy may require a private fact, intrusion or reasonable expectation of privacy. Copyright protects works, not the person as such. Passing off protects goodwill and consumer confusion. Criminal obscenity or intimate-image provisions protect only some sexualised harms. Generative AI collapses these categories because the artefact may be false, intimate, reputational, commercial and expressive at once.

A self-standing personality right supplies a direct answer: a person's face, voice, likeness and synthetic performance cannot be used for harmful synthetic identification without consent unless a recognised defence applies. It protects the celebrity whose voice is sold as a commercial model and the ordinary person whose face is inserted into intimate media, but it recognises that the former may claim licensing and goodwill loss while the latter may primarily claim dignity, safety, relational and employment harm.

Why the Right is Insufficient by Itself

The right becomes insufficient when treated as a private lawsuit. Ordinary victims face three structural barriers. The first is identification. AI identity harm often arrives through anonymous accounts, closed groups, reuploads, mirror sites and cross-border services. The second is cost. Urgent injunctions, expert reports and platform disclosure applications are expensive. The third is social risk. Filing a claim can amplify the content and expose the victim to shame, threats or retaliation.

United States and European intermediary cases show why platform involvement matters. Norwich Pharmacal relief developed to compel a third party mixed up in wrongdoing to disclose information needed to sue the wrongdoer (*Norwich Pharmacal Co. v. Customs and Excise Commissioners*, 1974). Website-blocking and intermediary-liability cases such as Cartier, L'Oreal v eBay and Google Spain show that legal systems already impose structured duties on intermediaries where private rights cannot be protected only against the original wrongdoer (*Cartier International AG v. British Telecommunications plc*, 2018; *Google Spain SL v. Agencia Española de Protección de Datos*, 2014; *L'Oréal SA v. eBay International AG*, 2011). Jurisdictional cases such as eDate Advertising also show that online personality harms raise cross-border forum questions from the outset (*eDate Advertising GmbH v. X*, 2011).

The Celebrity Ceiling

The celebrity ceiling is therefore not merely descriptive. It is a doctrinal risk. If the cause of action is built on passing off, it asks for goodwill. If it is built on publicity, it asks for commercial value. If it is built on defamation, it asks for reputational harm. If it is built on copyright, it asks for a work. Each gateway filters out part of ordinary identity harm. A self-standing personality right is needed precisely because those gateways are partial.

If the new right inherits only the enforcement habits of passing off, publicity and copyright, it will reproduce their hierarchy. The right must therefore recognise dignitary identity and commercial identity as distinct, cumulative interests. Market value may increase compensatory or disgorgement awards, but absence of market value cannot defeat liability, interim relief or damages for humiliation, loss of autonomy, safety risks, family consequences or disruption of work and education.

The distinction between commercial and dignitary identity must continue through liability and remedy. A false endorsement may justify lost-fee damages and disgorgement. A fabricated intimate image may have no market analogue but may justify urgent removal, anonymity, compensation for humiliation and safety costs, and orders preventing repeat distribution. A single market-value test would misclassify the second harm as legally minor.

Research Question Two: How Does Detection Bias Affect Proof, Equality and Access to Justice?

Data-protection law is relevant because biometric templates, facial geometry and voiceprints may be sensitive personal data when processed to identify a person. The GDPR's treatment of biometric data, access, erasure and automated decision-making offers useful comparative language even though Bangladesh requires its own statutory pathway (Regulation [EU] 2016/679, art. 9; Regulation [EU] 2016/679, arts. 15, 17, 22; Charter of Fundamental Rights of the European Union, 2012, arts. 7, 8, 11, 21).

The evidentiary lifecycle has four stages: discovery of the content, preservation of the content and associated metadata, assessment of synthetic provenance, and linkage to the claimant. The ordinary victim is least able to control the middle two stages. Platforms control logs, upload times, account connections and labelling data. Developers may control watermarking or provenance information. State forensic laboratories may control expert testing. Placing the full initial burden on the victim is therefore structurally irrational.

A fair evidence model would use graduated confidence. Low confidence should be enough for preservation where deletion would destroy the evidence. Medium confidence may justify temporary disabling where the risk of ongoing harm is high. High confidence should be required for final liability, damages or penalties. This staged approach avoids two extremes: denying help because early proof is imperfect, and imposing final sanctions on the basis of uncertain automated detection.

Detection bias also interacts with language hierarchy. English-language models, celebrity datasets and high-resolution entertainment media are more likely to be represented in training and evaluation. Bengali voice notes, compressed social-media clips and regional accents are less likely to be covered. The law should treat this as a predictable design issue. When regulators approve forensic tools, they should ask not simply whether the tool performs well on benchmark data, but whose data the benchmark represents.

The Bengali benchmark makes the burden problem concrete. The best zero-shot model reported 53.80% accuracy and a 46.20% equal-error rate, while language-specific fine-tuning improved accuracy to 79.17% and reduced the equal-error rate to 24.35% (Samu et al., 2025). Neither result is an appropriate gatekeeper for urgent protection. A victim facing a 53% accurate detector should not be required to obtain a better score before evidence is preserved. A sworn denial, comparison samples, contextual inconsistencies, witnesses, account history and the platform’s own metadata may establish the low threshold for preservation. The detector should be one item in a later, human-led assessment, with its limitations disclosed.

Detection as a Legal Gateway

The second research question is the article's central claim. Detection bias is not a downstream technical defect. It is a legal gateway. A claimant usually has to show that the contested content is synthetic, that it reproduces or imitates the claimant, and that the defendant or platform failed to take legally relevant steps. Each element may depend on forensic tools. If those tools are less reliable for Bengali speech, South Asian faces, women's faces or low-quality phone recordings, then legal protection becomes uneven before a judge reaches the merits.

This point changes the equality analysis. Equality before law does not mean that every claimant receives identical statutory words. It means that the legal system does not build proof conditions that predictably favour some groups over others. Bangladesh's Constitution guarantees equality before law and non-discrimination (Constitution of the People's Republic of Bangladesh, 1972, arts. 27-28). It also protects life and personal liberty (Constitution of the People's Republic of Bangladesh, 1972, art. 32). Article 39 protects speech but subjects it to reasonable restrictions (Constitution of the People's Republic of Bangladesh, 1972, art. 39). A deepfake statute that ignores unequal proof infrastructure would sit uneasily with these commitments, because it would make relief depend on technical systems whose errors are not equally distributed.

The Relation between AI Fairness and Legal Proof

AI fairness literature is often treated as policy background. In this field it is evidence law. A detector used to decide whether a platform takes down content, whether police investigate, whether a court grants interim relief, or whether a defendant is liable becomes part of the legal apparatus. If the detector lacks documentation, has not been tested on Bengali data, or has unknown demographic error rates, then reliance on it should be limited and carefully explained.

This does not mean that victims must wait for perfect detection. The opposite follows. Because detection is uncertain and unequally distributed, the law should not place the full burden on the victim at the first stage. A credible prima facie showing should trigger preservation, human review and platform disclosure. Expert proof can be refined later. The law should treat uncertainty as a reason to preserve evidence, not as a reason to abandon the complainant.

Content Provenance and its Limits

Content provenance systems may help but cannot replace remedies. The NIST AI Risk Management Framework encourages governance, mapping, measurement and management of AI risks (National Institute of Standards and Technology [NIST], 2024). C2PA and the Content Authenticity Initiative promote technical standards for content credentials and provenance (Coalition for Content Provenance and Authenticity [C2PA], 2026; Content Authenticity Initiative, 2026). These tools are valuable, but they are incomplete. Provenance can be stripped, absent, forged, or unavailable for legacy content. It also does not answer whether a platform acted reasonably after receiving notice of harm.

Therefore, detection and provenance should be treated as supporting evidence, not as exclusive gatekeepers. A Bangladesh statute should require platforms to preserve metadata and provenance signals where they exist, but it should not deny relief merely because a victim cannot produce a detector score. The legal test should combine victim evidence, contextual indicators, platform records, expert review and proportionality.

Graduated Evidence and Remedy Model

Table 1: A Graduated Evidence and Remedy Model

Stage	Threshold	Immediate action	Information burden	Speech safeguard
1. Preservation	Credible identity linkage and non-consent; no detector score required	Preserve content, metadata, logs and provenance signals	Platform produces records under its control after notice	No public removal required solely for preservation
2. Interim protection	Credible linkage plus serious risk of continuing or irreversible harm	Temporary disabling, de-indexing or prominent label; expedited review	Platform gives reasons and identifies automated tools used	Uploader notice, rapid human appeal and restoration if complaint fails
3. Final liability	Balance of probabilities based on the totality of evidence	Injunction, correction, damages, disgorgement and repeat-upload relief	Claimant proves core harm; defendant produces evidence for affirmative defence	Judicial decision, proportionality and appeal

This staged model aligns the level of proof with the reversibility and severity of the intervention. Preservation is minimally speech-restrictive and should occur early. Temporary disabling is more intrusive and therefore requires a credible risk of continuing serious harm plus rapid review. Final liability requires a full evidentiary record and permits the defendant to establish statutory defences.

Research Question Three: What Does India Show About the Promise and Limits of a Constitutional Route?

The Indian cases are best read as rapidly developing emergency jurisprudence. They provide urgent relief and increasingly speak in both commercial and dignitary terms, but the reported factual matrices remain dominated by prominent claimants, market substitution and large-scale online exploitation. This boundary does not weaken the cases. It identifies the next statutory task: translating their recognition of voice, likeness, autonomy and dignity into predictable procedures that an ordinary claimant can use.

For Bangladesh, the lesson is that constitutional dignity should be statutory translated. Courts can recognise identity harm case by case, but victims need predictable procedure before the first reported precedent. A statute can define the harm, assign platform duties, protect anonymity and set evidentiary standards. Without that translation, constitutional language may remain inspirational while remedies remain inaccessible.

Another Indian lesson concerns remedies against unknown defendants. John Doe or Ashok Kumar orders are attractive because synthetic identity harm often moves through anonymous accounts. Yet such orders can become too broad if they cover future, undefined speech. The better approach is targeted dynamic relief: the claimant should be able to add mirror links or

substantially identical harmful artefacts, but the order should preserve a route for contested expressive material to be reviewed.

Promise: Dignity, Autonomy and Speed

India demonstrates the promise of a constitutional and common-law route. *Justice K. S. Puttaswamy v. Union of India* (2017) supplies the language of dignity, autonomy and informational self-determination. The AI cases show that High Courts can grant ex parte relief, restrain unknown defendants and treat unauthorised voice and likeness imitation as legally cognisable. The 2026 decisions in *Varun Dhawan* and *Ravi Kishan* also show increasing judicial attention to AI-generated sexualised and inappropriate content, not only conventional endorsement markets.

The Indian route also shows that personality rights need not be reduced to property. Article 21 allows courts to speak in the language of personhood even when the immediate dispute involves commercial exploitation. Articles 14 and 15 can also support an equality analysis if synthetic identity harms fall more heavily on women or marginalised groups (Constitution of India, 1950, art. 14; Constitution of India, 1950, art. 15). This constitutional route is important because deepfake harm is not only market substitution. It is a non-consensual substitution of communicative agency.

Limit: Passing Off and Commercial Legibility

The remaining limit is fragmentation. Passing off and goodwill still do substantial work, while the Information Technology Act, Bharatiya Nyaya Sanhita and Copyright Act cover only parts of voyeurism, obscenity, defamation, performance and authorship. India's 2026 amendments to the Intermediary Guidelines introduced a definition of synthetically generated information, labelling and metadata duties, technical measures, shorter grievance timelines and special treatment for certain intimate impersonation complaints. This is meaningful platform-governance progress, but it is not a self-standing, automatic and dignity-based personality right for every individual, nor does it resolve unequal access to proof or independent review.

This is why India is both an inspiration and a warning for Bangladesh. It demonstrates that courts can stretch existing law toward AI identity protection. It also demonstrates that without statutory design, the protection will follow visibility, market value and legal capacity. The ordinary victim needs more than judicial creativity.

Lessons for Bangladesh

Bangladesh should therefore borrow the recognition that voice, likeness and synthetic performance are components of personal identity; the willingness to grant urgent and dynamic relief; and the emerging separation between commercial exploitation and dignitary injury. It should not import celebrity goodwill as the gateway to standing, or depend on executive control of content disputes.

The Indian experience also points to the need for procedural tools. Dynamic injunctions and John Doe orders can be useful when the same content migrates across sites. But they must be paired with safeguards: notice, time limits, judicial review, exceptions for public-interest expression and penalties for abusive complaints. Otherwise, the same machinery that protects victims can become a censorship device.

The comparison must also account for India's 2026 platform amendments. They show that rapid grievance handling, synthetic-content labelling and technical detection duties are administratively possible in South Asia. Bangladesh should adopt the useful procedural elements while adding stronger institutional independence, local-language audit and judicial review.

Research Question Four: What Remedial Architecture Should Bangladesh Adopt?

A platform-centred model must remain rights-respecting. Effective-remedy principles require accessible procedures, reasons, review and proportionality. Public authorities should not outsource final rights determinations to private platforms, and platforms should not be forced to remove contested public-interest speech permanently on the basis of an unreviewed automated score.

Bangladesh also requires institutional humility. Criminal prosecution should not be the default remedy for every AI identity wrong. Criminal law may be necessary for sexual exploitation, fraud, threats, election manipulation and repeat malicious conduct. But many cases require fast removal, correction, preservation and compensation rather than imprisonment. A civil-first architecture with reserved criminal escalation would reduce the risk of speech-control abuse while still treating severe harm seriously.

The institutional solution should be deliberately modest. A Digital Identity Remedy Cell should sit as a specialised service and registry unit within the National Legal Aid Services Organization, linked procedurally to designated civil or cyber benches and supervised by the judiciary. It should receive complaints, help preserve URLs and metadata, arrange initial technical triage, provide legal-aid referral, communicate notices to platforms and maintain anonymised statistics. It should have no power to declare general political speech unlawful, issue final blocking orders, or initiate criminal proceedings on its own. Final coercive orders should remain with courts, and every interim administrative step should be reasoned, time-limited and appealable.

Bangladesh should also avoid treating AI labelling as a complete answer. Labels are helpful when content is generated lawfully but may mislead viewers if unlabelled. They are less useful where malicious actors deliberately strip labels, where audiences do not see labels before sharing, or where the harm arises from the very existence of the synthetic performance. Labelling should therefore be one layer of a remedy system, not a substitute for removal, correction, preservation or compensation.

The statute should also address remedies after removal. Corrective notices, apology orders, disgorgement of profits, damages for dignitary harm and injunctions against repeat uploading serve different functions. Removal stops immediate circulation; correction addresses audiences already reached; damages recognise injury; disgorgement removes incentives; repeat-upload injunctions prevent recurrence. A single takedown remedy would be too narrow because identity harm continues through memory, screenshots, monetisation and reputational inference.

Constitutional Starting Point

Bangladesh should begin with constitutional balance. Articles 27 and 28 support equal access to protection. Article 32 supports dignity and personal liberty. Article 39 protects speech and therefore requires careful defences for journalism, satire, parody, research and public-interest archiving. The goal is not to criminalise every synthetic depiction. The goal is to stop non-

consensual synthetic identification that causes dignitary, sexual, economic, political or safety harm.

International human-rights law supports the same balance. The ICCPR protects privacy, expression and equality (International Covenant on Civil and Political Rights, 1966, arts. 17, 19, 26). General Comment No 34 stresses that restrictions on expression must be provided by law and necessary for a legitimate aim (U.N. Human Rights Committee, 2011). The UN Special Rapporteur's report on disinformation warns against overbroad state responses that undermine freedom of expression (U.N. Human Rights Council, 2021). A Bangladesh deepfake statute should therefore be precise, rights-based and remedy-focused, not a broad speech-crime instrument.

A Statutory Definition of AI Identity Harm

The statute should define AI identity harm as the non-consensual creation, distribution, monetisation or material amplification of synthetic or materially manipulated audio, image, video or interactive output that makes an identifiable person appear to speak, act, endorse, perform, appear nude or intimate, participate in political activity, or associate with a product, ideology or event in a manner that a reasonable viewer could treat as real or identity-linked. The definition should cover fully generated and substantially manipulated content, and it should make clear that fame, registration and commercial value are irrelevant to the existence of the right.

The statute should distinguish harmful synthetic identification from protected expression. Satire, parody, artistic transformation, journalism and public-interest research should remain protected where a reasonable audience is not deceived or where the public-interest justification outweighs the harm. This mirrors the logic of expressive-use cases and avoids making identity control absolute.

Platform-Side Duties

Platforms should provide an accessible identity-harm notice channel; preserve the file, upload data, account records and provenance signals immediately after a credible notice; conduct timely human review; temporarily disable access where severe or irreversible harm is plausible; prevent repeat uploading of a finally verified harmful artefact; notify the uploader; and publish aggregate transparency data. The United States' TAKE IT DOWN Act, whose platform-removal requirements took effect in May 2026, provides a useful implementation benchmark for rapid removal of non-consensual intimate images and known identical copies, although Bangladesh should retain a civil-first and judicially reviewable model (TAKE IT DOWN Act, 2025; Federal Trade Commission, 2026).

After a credible prima facie complaint, the burden of producing platform-controlled evidence should shift to the intermediary. The claimant should establish identity linkage, lack of consent and a plausible risk of harm. The platform should then produce available upload logs, labelling data, moderation history, provenance information and monetisation records. This is a burden of production, not an automatic presumption of final liability.

Evidence Rules and Forensic Fairness

Courts should grant preservation on a credible showing of identity linkage without requiring detector certainty. Temporary restriction should require both credible linkage and a serious risk of continuing or irreversible harm. Final liability should be decided on the balance of

probabilities from the totality of evidence. Expert reports should identify the detector, version, dataset coverage, language and demographic testing, error rates, compression sensitivity and whether the content has been edited or reuploaded. No detector output should be treated as conclusive by itself.

International AI-governance instruments support this audit approach. The OECD AI Recommendation, UNESCO Recommendation on AI Ethics and Council of Europe Framework Convention all emphasise human rights, transparency, accountability and risk management (Organisation for Economic Co-operation and Development [OECD], 2024; UNESCO, 2021; Council of Europe, 2024). Bangladesh can translate those principles into practical rules: no detector should be used as decisive legal evidence unless its limitations are disclosed, and no claimant should be denied urgent preservation merely because local-language detection is weak.

Victim Protection and Access to Justice

Complaints involving intimate, sexualised, religious, gendered, caste-related or retaliatory content should permit pseudonymous or anonymised case dockets, in-camera hearings, sealed or access-restricted exhibits, remote testimony where necessary, and rapid removal without requiring public reproduction of the material. These safeguards directly address the risk that litigation itself becomes a second publication of the harm.

Legal aid and administrative assistance are indispensable. The proposed Digital Identity Remedy Cell should operate under the National Legal Aid Services Organization rather than an executive cyber-security agency. A statutory advisory board should include judicial, technical, gender-harm, disability-access, child-protection and media-freedom expertise. Fixed functions, public procedures, independent audit, data minimisation and judicial appeal would reduce the risk that the cell becomes a censorship board.

Safe Harbours, Defences and Anti-Abuse Rules

The defence structure should allocate burdens explicitly. The claimant bears the initial burden of showing synthetic identification, lack of consent and plausible harm. Once the uploader or platform invokes consent, satire, parody, journalism, academic research, public-interest archiving, lawful investigation or transformative expression, that party bears the burden of producing evidence supporting the defence, because the relevant purpose, context and disclosure are ordinarily within its knowledge. The claimant retains the ultimate burden of proving unlawful identity harm on the balance of probabilities. At the interim stage, platforms should use labelling or temporary restriction where feasible, notify both parties and provide an expedited human appeal rather than treating an automated flag as a final decision.

India's amended Intermediary Guidelines show both the utility and risk of platform duties. Fast response and technical measures can protect victims, but vague standards and opaque automation can encourage over-removal. Bangladesh should therefore require reasons, notice, a record of automated tools used, accessible appeal, restoration when a complaint fails, and penalties for knowingly abusive notices. Safe harbour should depend on compliance with these procedures rather than unquestioning removal.

Remedies after Removal

Removal is only the first remedy. Courts should be able to order corrective notices delivered to substantially the same audience, de-indexing, disabling of monetisation, disgorgement of

profits, compensation for commercial and dignitary loss, reimbursement of counselling and safety costs, deletion of unlawfully retained biometric templates, and narrowly framed dynamic injunctions against verified identical or substantially equivalent reuploads. Corrective relief should be proportionate and should not compel admissions beyond what the evidence establishes.

Recommendations

The recommendations should be sequenced. Immediate reform should focus on preservation, reporting and victim protection, because these can reduce harm before a full AI statute is complete. Medium-term reform should build court procedure, platform duties and technical audit. Long-term reform should invest in local-language datasets, public forensic capacity and regional cooperation. This sequencing prevents the common mistake of passing broad offences first and building safeguards later.

A model statute should contain a three-year review clause, an independent equality and freedom-of-expression impact assessment, and public consultation. The review should examine new modalities such as real-time voice conversion, interactive avatars, agentic impersonation and synthetic live-streaming, while avoiding open-ended executive power to redefine offences.

Training is a separate recommendation because law on paper will fail without legal literacy among institutions. Judges need to understand detector uncertainty and platform logs. Police need protocols for preserving digital evidence without humiliating victims. Lawyers need pleadings that separate urgent preservation from final proof. Journalists need guidance on reporting synthetic media without amplifying harm. Schools and universities need media-literacy modules that teach students how to verify, report and resist synthetic impersonation.

First, Bangladesh should enact a narrow AI Identity Harm Act rather than add broad offences to general cyber-security law. The Act should define synthetic identity harm, identify civil remedies, provide urgent takedown and preservation powers, and avoid vague speech-crime language.

Secondly, the Act should create a two-stage proof model. At stage one, a credible prima facie showing should trigger preservation, temporary disabling in serious cases, and platform disclosure. At stage two, liability and final remedies should be determined after fuller evidence, including expert review and defences.

Thirdly, the Act should reverse the burden of evidence production after notice. Platforms and uploaders should disclose logs, labels, provenance signals, monetisation data and moderation history. Victims should not be forced to prove facts that only the intermediary can access.

Fourthly, Bangladesh should invest in Bengali and South Asian detection benchmarks. Public funding should support open evaluation datasets, independent auditing, and regular publication of error rates by language, gender and demographic group. A detector that has not been tested on Bengali speech or local facial data should not be treated as legally decisive.

Fifthly, the statute should protect complainant dignity. It should provide anonymity, confidentiality of intimate exhibits, fast removal of sexualised or retaliatory synthetic media, and penalties for doxxing complainants. The law should treat republication during proceedings as a separate harm.

Sixthly, Bangladesh should create a fast digital-identity procedure linked to designated civil or cyber benches. The service and triage function should sit within the National Legal Aid Services Organization, while preservation extensions, final takedown orders, damages and contested speech decisions should remain judicial. The procedure should be written, low-cost, evidence-preserving, capable of anonymised dockets and in-camera hearings, and subject to appeal.

Seventhly, the law should state both exceptions and burdens. After a prima facie showing by the claimant, a party relying on satire, parody, journalism, research, consent or public interest should produce evidence of that defence. The claimant should retain the ultimate burden of proving unlawful harm. Platforms should provide rapid interim review and restoration where an exception succeeds.

Eighthly, the law should require annual transparency reports from major platforms operating in Bangladesh. Reports should include identity-harm notices, action times, appeal outcomes, repeat-upload controls, use of automated detection and error audits. Aggregate reporting protects privacy while revealing whether the system works.

Ninthly, Bangladesh should create cross-border cooperation channels for disclosure and preservation. Many AI identity harms involve foreign platforms, offshore hosting and anonymous payment. Mutual legal assistance is too slow for first-stage preservation, so domestic law should impose local representative and preservation requirements for large platforms serving Bangladeshi users.

Tenthly, reform should be accompanied by media literacy and public guidance. Victims need to know how to preserve screenshots, URLs, timestamps and platform notices. Judges, police, lawyers and journalists need training on synthetic media, detection uncertainty and the difference between proof for urgent preservation and proof for final liability.

Conclusion

The result is a shift in the legal imagination. The question is not simply 'whose face does the law let you own?' but 'whose face can the legal system recognise, verify and protect in time?' Ownership language without remedy design is too thin. Effective remedy requires institutions that can act before viral spread becomes permanent, and evidence rules that do not punish victims for the technical limitations of systems they did not build.

In that sense, the article's proposal is not anti-technology. Detection tools, provenance systems and automated moderation can assist victims when they are documented, audited and used with human review. The objection is to making unequal technology the silent gatekeeper of equal rights. Law should use technical systems as evidence aids, not as constitutional substitutes. The final question for reform is therefore institutional: who checks the detector, who preserves the file, who hears the victim, and who reviews the platform's decision?

The central claim is that a personality right dependent on celebrity visibility, private litigation capacity and reliable detection is not universal. Indian courts and the 2026 intermediary amendments show important progress in recognising voice, likeness, synthetic sexualisation and platform responsibility. Yet the reported cases remain concentrated around prominent claimants, and procedural access, evidence preservation and detector fairness remain decisive for ordinary people.

Bangladesh shows why legal design must go further. The ordinary victim needs more than a right to sue. She needs evidence preservation, platform disclosure, anonymity, affordable procedure, detector fairness and speech-protective safeguards. Detection bias is therefore not an engineering footnote. It is a constitutional-equality problem, because proof systems decide whose harm the law can recognise.

The stronger architecture combines an automatic right triggered by synthetic identification with platform preservation and disclosure duties, graduated proof standards, anonymised and in-camera procedures, dignitary remedies independent of market value, audited local-language detection and clear public-interest defences. It would not eliminate AI identity harm, but it would move the law from symbolic ownership toward accessible, timely and reviewable protection for those whom current systems are least able to recognise (International Covenant on Civil and Political Rights, 1966, art. 2[3]; European Convention on Human Rights, 1950, art. 13).

REFERENCES

Aishwarya Rai Bachchan v. Aishwaryaworld.com & Others, CS(COMM) 956/2025 (Delhi High Court Sept. 9, 2025). https://delhihighcourt.nic.in

Amitabh Bachchan v. Rajat Nagi, 2022 SCC OnLine Del 4110 (Delhi High Court 2022).

Amnesty International. (2024). Repackaging repression: The Cyber Security Act and the continuing lawfare against dissent in Bangladesh. https://www.amnesty.org/en/documents/asa13/8332/2024/en/

Anil Kapoor v. Simply Life India & Others, CS(COMM) 652/2023 (Delhi High Court Sept. 20, 2023). https://delhihighcourt.nic.in

Arijit Singh v. Codible Ventures LLP, Interim Application (L) No. 23560 of 2024 in COM IPR Suit (L) No. 23443 of 2024 (Bombay High Court July 26, 2024). https://bombayhighcourt.nic.in

ARTICLE 19. (2025, June 18). Bangladesh: Defending free expression and electoral integrity in the digital age. https://www.article19.org/resources/bangladesh-defending-free-expression-and-electoral-integrity-in-the-digital-age/

Asha Bhosle v. Mayk Inc. & Others, Interim Application (L) No. 30382 of 2025 in COM IPR Suit (L) No. 30179 of 2025 (Bombay High Court Sept. 29, 2025).

Bangladesh Sangbad Sangstha. (2025, March 29). 410 cases over speech-based offences under cyber laws to be withdrawn. https://www.bssnews.net/news/259276

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104, 671-732.

Bharatiya Nyaya Sanhita, Act No. 45 of 2023 (India).

Bosher, H. (2026). Do deepfakes, digital replicas and human digital twins justify personality rights? Journal of World Intellectual Property. https://doi.org/10.1111/jwip.70020

Bradshaw, S., & Howard, P. N. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation. Oxford Internet Institute.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1-15.

Campbell v. MGN Ltd., [2004] UKHL 22.

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982.

Cardtoons, L.C. v. Major League Baseball Players Association, 95 F.3d 959 (10th Cir. 1996).

Cartier International AG v. British Telecommunications plc, [2018] UKSC 28.

Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

Chesney, B., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107, 1753-1820.

Chopra, P., Sony, R. A. L., & Chopra, S. (2025). Generative AI, copyright and personality rights: A comparative legal perspective. Legal Issues in the Digital Age, 6(3), 23-50.

Citron, D. K. (2019). Sexual privacy. Yale University Press.

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49, 345-391.

Coalition for Content Provenance and Authenticity. (2026). C2PA technical specification (Version 2.4). https://c2pa.org/specifications/specifications/2.4/index.html

Comedy III Productions, Inc. v. Gary Saderup, Inc., 25 Cal. 4th 387 (2001).

Constitution of India, 1950.

Constitution of the People's Republic of Bangladesh, 1972. https://bdlaws.minlaw.gov.bd/act-367.html

Content Authenticity Initiative. (2026). Content credentials. https://contentauthenticity.org/

Copyright Act, No. 14 of 1957 (India).

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Cyber Security Act, 2026 (Bangladesh). https://bdlaws.minlaw.gov.bd/

Deepa Jayakumar v. A. L. Vijay, AIR 2021 Mad 167 (Madras High Court 2021).

Digital Security Act, 2018 (Bangladesh).

DM Entertainment Pvt. Ltd. v. Baby Gift House, 2010 SCC OnLine Del 4790 (Delhi High Court 2010).

Douglas v. Hello! Ltd., [2007] UKHL 21.

eDate Advertising GmbH v. X, Joined Cases C-509/09 and C-161/10, EU:C:2011:685.

European Commission. (2026). Article 50: Transparency obligations for providers and deployers of certain AI systems. AI Act Service Desk. https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-50

European Convention on Human Rights, Nov. 4, 1950, 213 U.N.T.S. 221.

Federal Trade Commission. (2026). TAKE IT DOWN Act: What covered platforms need to know.https://www.ftc.gov/business-guidance/resources/take-it-down-act-what-covered-platforms-need-know

Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé, H., III, & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86-92. https://doi.org/10.1145/3458723

Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, EU:C:2014:317.

Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).

Human Rights Act 1998, c. 42 (UK).

Information and Communication Technology Act, 2006 (Bangladesh).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended 2026 (India). https://www.meity.gov.in/

Information Technology Act, No. 21 of 2000 (India).

International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

Ju, Y., Hu, S., Jia, S., Chen, G. H., & Lyu, S. (2024). Improving fairness in deepfake detection. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (pp. 4655-4665). https://openaccess.thecvf.com/content/WACV2024/html/Ju_Improving_Fairness_in_Deepfake_Detection_WACV_2024_paper.html

Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Supreme Court of India 2017).

Karttunen, S. (2026). The Danish approach to copyright and deepfakes: A model for the EU? European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf

Kaye v. Robertson, [1991] FSR 62.

Keller v. Electronic Arts, Inc., 724 F.3d 1268 (9th Cir. 2013).

Khan, D. (2026). Between criminalisation and governance: Regulating AI-generated deepfakes in Bangladesh's transitional democracy [Preprint]. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6508275

Krishna Kishore Singh v. Sarla A. Saraogi, (2021) 88 PTC 40 (Delhi High Court 2021).

Law Commission of England and Wales. (2022). Intimate image abuse: A final report (Law Com No. 407).

Livernoche, V., et al. (2025). Deepfakes in the 2025 Canadian election: Prevalence, partisanship, and platform dynamics [Preprint]. arXiv. https://arxiv.org/abs/2512.13915

L'Oréal SA v. eBay International AG, Case C-324/09, EU:C:2011:474.

Mahamuni, R. (2025). Lehrman and Indian celebs: How personality rights are getting real [Preprint]. SSRN.

Manila Principles on Intermediary Liability. (2015). https://www.manilaprinciples.org/

Marlan, D. (2025). Generative identity theft: Criminalizing deepfakes using the right of publicity. Akron Law Review, 58(3), 445-500.

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

Milmo, D. (2025, June 27). Denmark to tackle deepfakes by giving people copyright to their own features. The Guardian. https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence

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

Mitchell, M., et al. (2019). Model cards for model reporting. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 220-229). https://doi.org/10.1145/3287560.3287596

National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). https://doi.org/10.6028/NIST.AI.600-1

Norwich Pharmacal Co. v. Customs and Excise Commissioners, [1974] AC 133.

Online Safety Act 2023, c. 50 (UK).

Organisation for Economic Co-operation and Development. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Personal Data Protection Act, 2026 (Bangladesh). https://bdlaws.minlaw.gov.bd/

R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (Supreme Court of India 1994).

Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (pp. 429-435).

Ranka, H., et al. (2024). Examining the implications of deepfakes for election integrity [Preprint]. arXiv. https://arxiv.org/abs/2406.14290

Ravindra Shukla alias Ravi Kishan v. Ashok Kumar (John Doe), CS(COMM) 2026 (Delhi High Court July 2, 2026). https://delhihighcourt.nic.in

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act), 2022 O.J. (L 277) 1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), 2024 O.J. L 2024/1689.

Rini, R. (2020). Deepfakes and the epistemic backstop. Philosophers' Imprint, 20(24), 1-16.

Rogers v. Grimaldi, 875 F.2d 994 (2d Cir. 1989).

Samu, M. S. S., et al. (2025). Zero-shot to zero-lies: Detecting Bengali deepfake audio through transfer learning [Preprint]. arXiv. https://arxiv.org/abs/2512.21702

Santa Clara Principles on Transparency and Accountability in Content Moderation. (2021). https://santaclaraprinciples.org/

TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 50 (2025).

Tech Global Institute. (2024). Reforming AI laws and regulation in Bangladesh: Current harms and possible futures. https://techglobalinstitute.com/research/reforming-ai-laws-and-regulation-in-bangladesh-current-harms-and-possible-futures/

The Daily Star. (2026, July 7). Over 4.6 million cases pending in courts. https://www.thedailystar.net/

Transparency International Bangladesh. (2024). Review of proposed Cyber Security Rules, 2024. https://www.ti-bangladesh.org/

U.N. Human Rights Committee. (2004). General Comment No. 31: The nature of the general legal obligation imposed on States Parties to the Covenant (CCPR/C/21/Rev.1/Add.13).

U.N. Human Rights Committee. (2011). General Comment No. 34: Article 19, freedoms of opinion and expression (CCPR/C/GC/34).

U.N. Human Rights Council. (2021). Disinformation and freedom of opinion and expression: Report of the Special Rapporteur (A/HRC/47/25).

U.S. Copyright Office. (2024). Copyright and artificial intelligence, Part 1: Digital replicas. https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Varun Dhawan v. Artist Booking Company, CS(COMM) 2026 (Delhi High Court May 29, 2026). https://delhihighcourt.nic.in

Waits v. Frito-Lay, Inc., 978 F.2d 1093 (9th Cir. 1992).

Wasi, A. T., et al. (2025). Seeing isn't believing: Addressing the societal impact of deepfakes in low-tech environments [Preprint]. arXiv. https://arxiv.org/abs/2508.16618

Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11), 39-52.

White v. Samsung Electronics America, Inc., 971 F.2d 1395 (9th Cir. 1992).

World Intellectual Property Organization. (2025, April 17). AI voice cloning: How a Bollywood veteran set a legal precedent. WIPO Magazine. https://www.wipo.int/en/web/wipo-magazine/articles/ai-voice-cloning-how-a-bollywood-veteran-set-a-legal-precedent-73631

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